2008-12-01

An Operational Utility Assessment: Measuring the Effectiveness of the Joint Concept Technology Demonstration (JCTD), Joint Forces Protection Advance Security System (JFPASS)

NPS-LM-08-118

ACQUISITION RESEARCH SPONSORED REPORT SERIES

An Operational Utility Assessment: Measuring the Effectiveness of the Joint Concept Technology Demonstration (JCTD), Joint Forces Protection Advance Security System (JFPASS)

03 December 2008

by

Mark McGovern, MAJ, USA

Joseph Symmes, LCDR, USN, and

Jeffrey D. Mayor, LCDR, USN

Advisors: Dr. Daniel Nussbaum, Professor, and

Raymond Franck, Senior Lecturer

Graduate School of Business & Public Policy

Naval Postgraduate School

Prepared for: Naval Postgraduate School, Monterey, California 93943

ACQUISITION RESEARCH PROGRAM
GRADUATE SCHOOL OF BUSINESS & PUBLIC POLICY
NAVAL POSTGRADUATE SCHOOL

The research presented in this report was supported by the Acquisition Chair of the Graduate School of Business & Public Policy at the Naval Postgraduate School.

To request Defense Acquisition Research or to become a research sponsor, please contact:

NPS Acquisition Research Program
Attn: James B. Greene, RADM, USN, (Ret)
Acquisition Chair
Graduate School of Business and Public Policy
Naval Postgraduate School
555 Dyer Road, Room 332
Monterey, CA 93943-5103
Tel: (831) 656-2092
Fax: (831) 656-2253
e-mail: jbgreene@nps.edu

Copies of the Acquisition Sponsored Research Reports may be printed from our website www.acquisitionresearch.org

ACQUISITION RESEARCH PROGRAM
GRADUATE SCHOOL OF BUSINESS & PUBLIC POLICY
NAVAL POSTGRADUATE SCHOOL

Abstract

Planning modern military operations requires an accurate intelligence assessment of potential threats, combined with a detailed assessment of the physical theater of operations. This information can then be combined with equipment and manpower resources to set up a logistically supportable operation that mitigates as much of the enemy threat as possible. Given such a daunting challenge, military planners often turn to intelligent software agents to support their efforts. The success of the mission often hinges on the accuracy of these plans and the integrity of the security umbrella provided.

The purpose of this project is to provide a comprehensive assessment of the Joint Forces Protection Advanced Security System (JFPASS) Joint Concept Technology Demonstration (JCTD) to better meet force-protection needs. It will also address the adaptability of this technology to an ever-changing enemy threat by the use of intelligent software. This project will collect and analyze data pertaining to the research, development, testing, and effectiveness of the JFPASS and develop an operational effectiveness model to quantify overall system performance.

Keywords: Joint, Protection, Security, Fusion, Interoperable, BCA, CBRN, Force Protection, System-of-systems, Intelligent, Software, Agents, Context, COTS, Fusion

THIS PAGE INTENTIONALLY LEFT BLANK

Acknowledgements

First and foremost, the group would like to thank our advisors, Prof. Dan Nussbaum and Prof. Raymond (Chip) Franck, for their tireless efforts in helping us complete our project. Their advice and guidance were key in making this project a success.

MAJ Mark McGovern would like to thank his fellow group members for their hard work and relentless efforts to ensure project completion. He would also like to thank his wife for her understanding of long hours after school and late nights during this process. Her support was instrumental in the mental and physical drive that sustained the journey to success. He would also like to thank his children for their tireless efforts to delete the entire project from his home computer in an attempt to see what all those buttons do that daddy uses all the time.

LCDR Joe Symmes would like to thank both Mark and JD for their contributions to this project. The group worked extremely well together, each member pulling the load in his area of expertise. He would also like to thank his wife and children for their support and encouragement through the long hours of research and writing.

LCDR J.D. Mayor would to thank Mark and Joe for their tireless efforts and devotion to mission accomplishment. He would also like to thank Prof. Nussbaum and Prof. Franck for their support in helping complete the project. Also, a special thank you goes to his family.

The team would also like to thank the JFPASS team for their support and all the information and time given to this project.

THIS PAGE INTENTIONALLY LEFT BLANK

About the Authors

MAJ Mark McGovern, United States Army, is currently a student in the Master of Business Administration program (with an emphasis on Supply Chain Management) at the Naval Postgraduate School, Monterey, California. MAJ McGovern completed his undergraduate studies at Virginia Tech in Blacksburg, Virginia. Prior to his current assignment, MAJ McGovern served as the Operations Officer for the Group Support Battalion, 7th Special Forces Group, located at Fort Bragg, North Carolina. His next duty assignment is to 1st Theater Sustainment Command, Fort Bragg, North Carolina.

LCDR Joseph Symmes, United States Navy, is currently a student in the Master of Business Administration program (with an emphasis on Supply Chain Management) at the Naval Postgraduate School, Monterey, California. LCDR Symmes completed his undergraduate studies at the United States Naval Academy in Annapolis, Maryland. Prior to his current assignment, LCDR Symmes served as the Supply Officer for the USS OGDEN (LPD-5) homeported in San Diego, California. His next duty assignment is to the US Transportation Command, Scott Air Force Base, Illinois.

LCDR Jeffery D. Mayor, United States Navy, is currently a student in the Master of Business Administration program (with an emphasis on Supply Chain Management) at the Naval Postgraduate School, Monterey, California. LCDR Mayor completed his undergraduate studies at San Diego State University in San Diego, California. Prior to his current assignment, LCDR Mayor served as the Supply Officer for the USS McCAMPBELL (DDG-85) homeported in San Diego, California. His next duty assignment is to Navy Expeditionary Logistics Support Group, Williamsburg, Virginia.

THIS PAGE INTENTIONALLY LEFT BLANK

NPS-LM-08-118

ACQUISITION RESEARCH SPONSORED REPORT SERIES

**An Operational Utility Assessment:
Measuring the Effectiveness of the Joint Concept Technology Demonstration (JCTD), Joint Forces Protection Advance Security System (JFPASS)**

03 December 2008

by

Mark McGovern, MAJ, USA

Joseph Symmes, LCDR, USN, and

Jeffrey D. Mayor, LCDR, USN

Advisors: Dr. Daniel Nussbaum, Professor, and

Raymond Franck, Senior Lecturer

Graduate School of Business & Public Policy

Naval Postgraduate School

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

THIS PAGE INTENTIONALLY LEFT BLANK

List of Abbreviations and Acronyms

ACC	Air Combat Command
ACTD	Advance Concept Technology Demonstration
ADUSD (AS&C)	Assistant Deputy Undersecretary of Defense (Advanced Systems and Concepts)
ADM	Acquisition Decision Memorandum
AI	Artificial Intelligence
AO	Area of Operation
APB	Acquisition Program Baseline
ATEC	US Army Test and Evaluation Command
ATO	Authority to Operate
BCA	Business Case Analysis
C&A	Certification and Accreditation
CBA	Capabilities-based Assessment
CCB	Configuration Control Board
CCTV	Closed-circuit Television
CD	Compact Disk
CDD	Capability Development Document
CBRNE	Chemical, Biological, Radiological, Nuclear and Explosive
COCOM	Combatant Commands
COI	Critical Operational Issues
CONEMP	Concept of Employment
CONOPS	Concepts of Operations
CONUS	Continental United States
COP	Common Operational Picture
COTS/GOTS	Commercial Off-the-shelf/Government Off-the-shelf
CPM	Capability Portfolio Manager
CRB	Candidate Review Board
DIACAP	DoD Information Assurance Certification Accreditation Process

DoD	Department of Defense
DOTMLPF	Doctrine, Organization, Training, Materiel, Leadership, Personnel, and Facilities
DSS	Decision Support System
ECP	Entry Control Point
ECPS	Entry Point Control System
EU	Extended Use
FCB	Functional Capability Boards
FOB	Forward Operating Base
FP	Force Protection
FPCON	Force Protection Condition
FPJE	Force Protection Joint Experiment
FY	Fiscal Year
GAO	Government Accountability Office
GIS	Geospatial Information Systems
GPS	Global Positioning System
GSR	Ground Surveillance Radar
GWOT	Global War on Terror
IA	Integration Assessments
IAP	Integrated Assessment Plan
IATO	Interim Authority to Operate
IC	Interim Capability
ICD	Initial Capabilities Document
ICD	Interface Control Document
IED	Improvised Explosive Devices
IEEE	Institute of Electrical and Electronics Engineers
IFF	Identification Friend or Foe
IGSSR	Integrated Ground Security Surveillance and Response
ILD	Integrated Locking Device
IPP	Installation Protection Program
IPP	Internet Protocol
ISSM	Information Systems Security Manager

IUBIP	Integrated, Unit, Base, and Installation Program
JBC2S	Joint Battlespace Command and Control System
JCIDS	Joint Capability Integration Development System
JCTD	Joint Capabilities Technology Demonstration
JCS	Joint Chiefs of Staff
JE	Joint Experimentation
JFCA	Joint Functional Capability Area
JFCOM	Joint Forces Command
JFPASS	Joint Force Protection Advanced Security System
JPEO-CBD	Joint Program Executive Office—Chemical Biological Defense
JPMG	Joint Project Manager Guardian
JSSG	Joint Service Steering Group
KSA	Knowledge, Skills and Abilities
C2	Command and Control
LCC	Lifecycle Cost
LOC	Lines of Communication
LOUA	Limited Operational Utility Assessment
LRIP	Low-rate Initial Production
MAA	Mission Area Analysis
M&S	Modeling and Simulation
MANPADS	Man-portable Air Defense Systems
MANSCEN	Maneuver Support Center
MDARS	Mobile Detection Assessment and Response System
MIPR	Military Interdepartmental Purchase Requests
MOE	Measure of Effectiveness
MOP	Measure of Performance
MTP	Management and Transition Plan
NNMSA	Non-nuclear Material Storage Area
NPS	Naval Postgraduate School
OD	Operational Demonstration
OGA	Other Government Agency

OIS	Office of Intelligence and Security
OM	Operational Manager
OSD	Office of the Secretary of Defense
OTD	Open Technology Development
OUA	Operational Utility Assessment
OV-1	Operational View -1
PBIED	Personnel-borne Improvised Explosive Devices
PE	Program Element
POC	Point of Contact
POG	Practical Operating Guidance
POM	Program Objective Memorandum
POR	Programs of Record
PPBE	Planning, Programming, Budgeting, and Execution
PSA	Program Support Agreement
PSDS2	Persistent Surveillance and Dissemination of Systems
PSEAG	Physical Security Equipment Action Group
QRF	Quick Reaction Force
QTR	Quarter
RAM	Rockets, Artillery, and Mortar
REF	Rapid Equipping Force
RF	Radio Frequency
ROC	Regional Operations Center
ROWS	Remotely Operated Weapon Systems
RPG	Rocket-propelled Grenades
S&T	Science and Technology
SAMP	Simplified Acquisition Management Plan
SDD	Systems Development and Demonstration
SEIWG	Security Equipment Interface Working Group
SETA	Scientific, Engineering, and Technical Assistance
SF	Special Forces
SIPRNET	Secret Internet Protocol Router Network
SME	Subject-matter Experts

SOF	Special Operations Forces
SOFA	Status of Forces Agreements
SSAA	Systems Security Accreditation Agreement
SSCG	System Security Classification Guide
SV	System View
TASS	Tactical Automated Security System
TD	Technical Demonstration
TI	Technology Integrator
TM	Technical Manager
TRL	Technology Readiness Levels
TTA	Technology Transition Agreement
TTP	Tactics, Techniques, and Procedures
UAV	Unmanned Aerial Vehicles
UGS	Unattended Ground Sensors
UGV	Unmanned Ground Vehicles
USAFE	United States Air Forces Europe
USEUCOM or EUCOM	United States European Command
VBIED	Vehicle-borne Improvised Explosive Devices
VMD	Video Motion Detection
XM	Transition Manager
YOE	Year of Execution
ZBV	Z Backscatter Van

THIS PAGE INTENTIONALLY LEFT BLANK

Executive Summary

As of this writing, the Joint Force Protection Advanced Security System (JFPASS) Joint Capability Technology Demonstration (JCTD) is the newest initiative of this type and is sponsored by the Office of the Secretary of Defense (OSD). The goal of the JFPASS is to find a common core of communication protocols that will bring interoperability of legacy and future force protection systems in order to provide a better means of perimeter security. “The Army is the lead service in this endeavor and has provided the Transition Manager (XM). The Navy provided the Technical Manager (TM), and the US European Command (EUCOM) has provided the Operational Manager (OM)” (Guardian Six, 2008, July 11).

The JFPASS supports the Global War on Terror (GWOT) by providing Combatant Commands (COCOMs), services, agencies and our allies with near-real-time, integrated/interoperable, comprehensive land and maritime-based regional and local Force Protection (FP) systems to counter threats. This is a precedent-setting solution to joint FP (2008, July 11).

The JFPASS integrates Chemical, Biological, Radiological, Nuclear, and Explosive (CBRNE) and Physical Security systems through the application of an integrated Command and Control (C2) Architecture that uses tailored decision rules. The JFPASS provides actionable information and allows users to focus on arriving at the appropriate decisions. The JFPASS JCTD architecture consists of nodes that together constitute a suite of sensors. These nodes are connected to a C2 system—rather than sensors connected directly to a C2 system (2008, July 21). Although the JFPASS is capable of connecting directly to sensors, the strength of the system is its ability to integrate legacy, existing, and emerging systems (2008, July 21). Using intelligent software as the enabling agent, JFPASS will provide the integration for the C2 Architecture and will provide the next evolution of technology information.

Current technologies, CONOPS, and policies do not provide a comprehensive, effective, and sustainable joint force protection capability. Fielded force protection systems do not interoperate and integrate effectively nor do they provide comprehensive and integrated situational awareness. Existing service stovepipe systems need to be joined into a single, integrated FP system-of-systems. The JFPASS has the potential to enhance FP using unmanned systems, integration fusion, and analysis software systems; this means actionable information can be presented in a timely manner, allowing the warfighter (WF) to focus on orchestrating responses such as deploying Quick Reaction Forces (QRFs). The JFPASS can also provide cost savings through standardization and effective use of manpower (2008, July 11).

I. Introduction

A. Overview

This report presents an overview of the need for increased FP. With a growing list of adversaries, including hostile states and transnational terrorist organizations, the nature of warfare has changed. Accordingly, US forces have shifted from a command-and-control model to a sense-and-respond model (Lin, Luby, & Wang, 2004, December, p. 26). Since the US Department of Defense (DoD) must respond to threats against American citizens or the military, it continuously explores new technologies to field capable force protection equipment.

As the largest defense organization in the free world, the DoD recognizes the need for the safety and protection of its fighting forces. The Joint Force Protection Advance Security System (JFPASS) can improve current FP to a highly effective level. It is centered on integrating communication protocols and applying commercial off-the-shelf (COTS) technologies to provide superior force protection capability in and around Forwarding Operating Bases (FOBs).

For the purpose of this report, an FOB is any secured forward position that is used to support tactical operations. An FOB may contain an airfield, hospital or other facility, and it may or may not be used for an extended period of time. FOBs are traditionally supported by main operating bases. For example, an FOB can reduce reaction time and increase time-on-task in deploying a patrol force. In its most basic form, an FOB consists of a ring of barbed wire around a position with a fortified entry control point (ECP). More advanced FOBs include assemblies of earthen dams, concrete barriers, gates, watchtowers, bunkers and other force protection infrastructure (Forward operating base, 2008).

B. Background

In the course of this project, the team conducted a literature review. The background provides the foundation regarding problems in the DoD's communication and interoperability of force protection systems. Also, the project will show how potential solutions to this problem are being assessed through the JCTD process.

C. Problem Statement

As the *JFPASS JCTD Management and Transition Plan* explains, "Currently, U.S. Joint and coalition FP systems are inadequate and lack the ability to provide comprehensive, effective sustainable FP and critical asset protection capabilities" (Guardian Six, 2008, July 11). The researchers in this study will assess the JFPASS as a solution to this problem.

D. Research Questions

Our primary aim is to help assess the extent to which the JFPASS can increase ability to enhance joint service force protection against an adaptive threat. The project will focus on the following research questions:

- How do the services operate with current security measures and actions, and is there a robust adaptability to changing threats?
- What types of management structures are used to assess security measures? Are they contracted services?
- What types of training are required for Force Protection (FP) personnel to operate and/or implement within the joint forces community when received?
- To what extent do the respective military services acquire and manage force protection equipment/services separately? Is this beneficial to the DoD acquisition strategy?
- To what extent can the JFPASS assist in preventing military and civilian causalities?

- What benefits does the JFPASS provide relative to what is already used?
- What is the "force protection" model used to design the JFPASS?
- Is the JFPASS a single-scenario design (e.g., expeditionary units like SEALS, Rangers, or LRSC)? Or is it designed for a broad range of applications?

E. Benefits of Research

The JFPASS has the potential to facilitate a more efficient use of resources both operationally and logistically. Specifically, this research project will:

- Support an assessment of the suitability of the JFPASS JCTD for transition to a Program of Record (POR),
- Contribute to a comprehensive understanding of joint force protection acquisition and of the adaptability of the force protection means currently in use,
- Provide information that can be incorporated into recommendations for future force protection acquisitions by means of intelligent software,
- Assess the utility of the JFPASS concept of COTS interoperability, and
- Investigate the possibility of future uses of the JFPASS in homeland defense against possible terrorist activities.

F. Methodology

For this project, we used an exploratory case study as our primary methodology. We employed a triangulation method to gather qualitative data. Three points were considered: interviews of JFPASS JCTD program representatives, relevant publications, and an exploratory survey of force protection reports. We used the survey to map five key force protection tasks to eight desired capabilities in order to asses the relative importance of each capability from an operations' perspective. Data gathered from the survey was

used to build a utility function as a metric for the JFPASS's operational capability. The research team believes the following areas pose the greatest problems in FP at present: (1) adaptability (speed), (2) interoperability (plug-and-play), and (3) effectiveness. We address each in our analysis.

II. Background

A. Current Problem

The terrorist attacks of September 11, 2001, resulted in a renewed interest in FP. A variety of new products—ranging from fire-resistant clothing to unmanned aerial vehicles—received serious DoD attention. The challenge is now in the integration of the available products into one cohesive and adaptable system.

Base defense is a key component of the force protection mission. The *JFPASS JCTD Management and Transition Plan* explains:

> The problem is the result of outdated capabilities, Concept of Operations (CONOPS) and policies. The excessive variants and redundancies in FP capabilities limit the Joint Force in its ability to share information across the services, agencies and partner nations. The outdated information and data exchange standards also limit the ability of the services, agencies and our partner nations to share and exchange data in order to maintain situational awareness of an ever vigilant and changing threat. The myriad of FP systems and inconsistent standards between systems severely limit their ability to communicate warnings rapidly from a single node to subordinate units and commands throughout the services and agencies. The limited interoperability between the various systems increases the total cost of ownership for FP systems due to inefficient manpower utilization and the high cost of maintaining multiple systems and spare parts. The current problem causes an unacceptable level of risk for critical and sensitive asset protection as well as unaffordable costs associated with operating and maintaining these different systems. (2008, July 11)

However, the technology development response has been sluggish thus far. BG Phillip Coker, Director of Capabilities Developments at the Futures Center at Army Training and Doctrine Command, states, “It is important to think through and find the right solutions, not solve the wrong problem” (Roosevelt, 2004, June 3, p. 1). In order to do so, the US must focus our efforts on a systematic approach to finding and implementing the right solutions to real-world problems with the right degree of force protection.

B. Current DoD Force Protection Guidance

Since September 11, 2001, the DoD has been proactive in protecting its infrastructures and personnel from acts of terrorism. *DoDI 2000.16* addresses the DoD's antiterrorism (AT) standards and is applicable to the Office of the Secretary of Defense (OSD), Military Departments, Chairman of the Joint Chiefs of Staff, Combatant Commands, Defense Agencies, DoD Field Activities, and all other DoD organizational entities (DoD, 2006, October 2, p. 2). The Instruction further addresses the DoD's policy and responsibilities as follows:

> 1. To protect DoD personnel, their families, installations, facilities, information, and other material resources from terrorist acts;
>
> 2. To establish AT standards for the Department of Defense;
>
> 3. That commanders at all levels shall have the authority to enforce security measures and are responsible for protecting persons and property subject to their control;
>
> 4. That Geographic Combatant Commander AT policies and programs shall take precedence over all AT policies or programs of any DoD Component operating or existing in that command's area of responsibility (AOR) except for those under the security responsibility of a Chief of Mission (COM);
>
> 5. That the DoD elements and personnel not falling under the AT policies and programs of a geographic Combatant Commander […], shall comply with the Overseas Security Policy Board Security Standards;
>
> 6. That non-DoD tenants on a DoD installation, facility, or other DoD property must comply with all aspects of the DoD AT program addressed in this Instruction and other AT guidance documents; and
>
> 7. That functional Combatant Commanders will support geographic Combatant Commanders as they exercise overall AT responsibility within their AOR. (2006, October 2, p. 2)

C. Force Protection Conditions

DoD Force Protection Conditions (FPCONs) is a DoD-approved system that standardizes security measures to protect US personnel and facilities from

terrorist attacks. The five progressive FPCON levels of force protection are listed below:

1. **FPCON NORMAL:** Applies when a general global threat of possible terrorist activity exists and warrants a routine security posture. At a minimum, access control will be conducted at all DoD installations and facilities.

2. **FPCON ALPHA:** Applies when there is an increased general threat of possible terrorist activity against personnel or facilities, and the nature and extent of the threat are unpredictable. ALPHA measures must be capable of being maintained indefinitely.

3. **FPCON BRAVO:** Applies when an increased or more predictable threat of terrorist activity exists. Sustaining BRAVO measures for a prolonged period may affect operational capability and military-civil relationships with local authorities.

4. **FPCON CHARLIE:** Applies when an incident occurs or intelligence is received indicating some form of terrorist action or targeting against personnel or facilities is likely. Prolonged implementation of CHARLIE measures may create hardship and affect the activities of the unit and its personnel.

5. **FPCON DELTA:** Applies in the immediate area where a terrorist attack has occurred or when intelligence has been received that terrorist action against a specific location or person is imminent. This FPCON is usually declared as a localized condition. FPCON DELTA measures are not intended to be sustained for an extended duration. (DoD, 2006, October 2, p. 39)

Each FPCON level encompasses site-specific AT security measures. FPCON protective measures are used to assist DoD components in reducing the risks of terrorist attacks and other security threats to DoD personnel, units, and activities (2006, October 2, p. 39). Upon declaration of an FPCON level, commanders are responsible to immediately implement all applicable AT security measures for that FPCON level unless the requirement is waived in writing by a

competent authority (2006, October 2, p. 40). Baseline FPCON levels and applicable measures are listed in Enclosure 4 of *DoDI 2000.16*. The instruction lists shipboard security measures separately; these are tailored to assist commanding officers and ship masters in reducing the effect of terrorist and other security threats to DoD combatant and non-combatant vessels—including US Army and Military Sealift Command ships worldwide (2006, October 2, p. 40).

D. What is a JCTD?

This Joint Capability Technology Demonstration (JCTD) Program has entered its third year of exploring new ways to provide a greater advantage against changing threats. The following is an excerpt from the JCTD Program Practical Operating Guidelines (POG) (DoD, 2008, April 11):

> The Joint Capability Technology Demonstration (JCTD) Program attempts to improve turnaround time from operational problem identification to operational capability. The Deputy Under Secretary of Defense for Advanced Systems and Concepts (DUSD [AS&C]) initiated the JCTD program in 2006 as a result of a top-down review of the Advanced Concept Technology Demonstration (ACTD) Program. In Fiscal Year (FY) 2006, the DUSD (AS&C) initiated the JCTD Program to enhance and accelerate the support to the joint, coalition and interagency WF's and users in this era of the global war on terrorism.

In that regard, the JCTD model is oriented to fill specific warfighter (WF) needs. Application of the model is an effective method for the DoD to fill requirements by emphasizing a "needs pull" over a "technology push" methodology, as the following statements attest (US DoD Announces, 2008, January 30):

- A JCTD enables faster project start-up by providing more resources earlier in the traditional two-year DoD budget cycle and a flexible start process that facilitates urgently needed combatant command-driven capabilities throughout the fiscal year.
- A key aspect of the JCTD program is the transition planning process, which seeks to deliver enduring capabilities to the combatant commands.

- The JCTD program also demands faster fielding of interim capabilities [and] structures funding to provide incentives for military service and agency participation without requiring the services or agencies clear visibility in their participation of joint efforts. (2008, January 30)

- The JCTD model seeks the 70%–80% solution now, rather than delaying delivery to obtain the 100% answer years from now (DoD, 2008, April 11). The advantage the JFPASS gains from the JCTD model is the streamlining process and utilization of current technologies to meet the 70%–80% objective.

E. What is the JFPASS?

The JFPASS is the "fusion cell" of a Command and Control software suite designed to create the interoperability of numerous COTS, enhancing FP for an array of units. This will allow all branches of the US military to harness the benefits of one joint force protection system. Intelligent software is the primary means in which the JFPASS intends to accomplish providing the enhanced FP.

1. Scope of the JFPASS JCTD

One recent article (US DoD announces, 2008, January 30) elaborates on the scope of the JFPAS system:

> JFPASS—integrates and automates access control and perimeter security for expeditionary military installations. JFPASS demonstrates an integrated system-of-systems to protect expeditionary military installations, incorporates comprehensive situational awareness for force protection providers, reduces manning due to systems integration and robotics, and reduces logistics cost. Functional areas for installation protection addressed include: perimeter security, chemical-biological-radiological defense, access control, nonintrusive inspection, and waterside security. (p. 2)

2. What the JFPASS Provides

This same article explains the benefits the system is expected to provide:

> JFPASS JCTD will provide improved situational awareness to protect humans from unnecessary risks, and facilitate the processes of detecting, assessing, warning, defending, and restoring a normal operational

capability. The focus will be on the response within Detect, Assess, and Warn functions. Enablers for response are the COP and the use of connected Unattended Ground Sensors (UGS) and unmanned systems, through the integration of legacy systems and automated responses. (2008, January 30, p. 2)

Figure 1. Desired Capabilities Provided by the JFPASS
(Guardian Six, 2008, July 11)

As seen in Figure 1, the JFPASS has the potential to bring protection support from fort to foxhole by providing next-generation passive capabilities (Guardian Six, 2008, July 11). In order to accomplish this, the JFPASS will have to incorporate new technology—not just hardware but software as well.

According to Mr. Carlos Lama, the JFPASS JCTD Program Manager, current "force protection systems are disjointed and inefficient" (2008, July 21). His statement affirms the need for a joint security system that can be used anywhere by any branch in austere locations against an unknown threat. Additionally, the DoD recognizes that current force protection technologies do not provide a comprehensive, effective, and sustainable joint force protection capability (2008, July 21). Current systems create waste through redundancy

and misuse of limited manpower and, therefore, do not provide the situational awareness needed by the WF (2008, July 21). Prior to this JCTD, there was no indication of a systematic approach to address such shortfalls.

The lack of a future DoD force protection vision has been a barrier to resolving such a problem. The Army is keenly aware of this problem: "Gen. Peter Schoomaker, Army Chief of Staff, tasked his subordinates to find science and technology solutions for the current and future force gaps and, where possible, accelerate fielding of future capabilities to improve current force effectiveness" (Roosevelt, 2004, June 3, p. 1). Disjointed supply lines and maintenance/repair capabilities also fragment the effectiveness of current force protection equipment issued to WFs.

Interoperability is an essential element in the success of any system designed to defeat a changing threat. The needs to reduce risk, increase effective Command and Control (C2) and reduce cost are catalysts for the development of the JFPASS for base defense. However, interoperability and the aforementioned elements are not the sole considerations. Speed is also a key element in the development of the JFPASS. Speed in set-up, becoming operational, break-down, and transport are essential to the light, elite units that will find this system most useful. Is there a speed versus interoperability trade-off that needs to be addressed? This is a question that must be answered by the WF.

In their December 2007 NPS study, D'Angelo, Houglan, and Ruckwardt state:

> Service components are responsible to train and equip the WF while geographical combatant commands conduct military wartime contingency operations. Each service provides trained and equipped forces to the combatant commanders—giving the commanders the capability to execute contingency operations. Although these capabilities consist of each service's core competencies, the combatant commanders are left with a void that only can be filled by external resources. (p. 4)

Agencies outside the DoD need to conduct research and development of technology that can provide systems to keep the military ahead of its adversaries and the US safe by filling that void. Exploring intelligent software to alleviate some of the burden placed on manpower can assist in this problem.

F. The Purpose of the JFPASS

The JFPASS can potentially fill a national force protection need. Its adaptability may be broad enough to allow an application to homeland defense applications as well as military perimeter security.

As stated in the overview, the overriding objective of this project is to analyze the effectiveness and adaptability of the JFPASS in defeating the ever-changing enemy threat. This project will investigate, analyze and assess the JFPASS. In addition, this project will provide the basis for our recommendation and assessment of the potential of the JFPASS to become a program of record.

G. Five Tasks of the JFPASS

The following five FP tasks are key elements to the system effectiveness of the JFPASS, according to the *JFPASS JCTD MTP* (Guardian Six, 2008, July 11):

1. **Detect:** The JFPASS will demonstrate the ability to detect threats using an integrated system of sensors (including cameras, radar, and CBRNE detection) and automated anomaly detection and alarming; these capabilities will reduce the need for human interaction with the system and will provide consistent detection probability results. The synergistic effect between sensor data and the JFPASS fusion engine will result in an improved response both in the time required to recognize a threat and the ability to do so at greater distances from vital assets.

2. **Assess:** The JFPASS will integrate the sensors into an automated, centrally controlled processing station(s), which will evaluate the input from each of the sensor systems. The JFPASS will automate the assessment process by comparing the nature of any anomaly detected by the system to the current understanding

of any known threat; by doing so, it will assess the potential for the anomaly to become a threat (i.e., presence of explosive components or precursors). The JFPASS will then automatically provide the system operator with recommended courses of action.

3. **Warn:** The JFPASS will automate the process of disseminating alerts and warnings over a multi-tiered/multi-mode communications system—ranging from loud speakers to automated emails and text messages. The system will provide situational awareness and information for decision-makers. An inter-networked system of the JFPASS-enabled units, bases and installations will disseminate warnings in order to mitigate the effects of dispersed, coordinated attacks.

4. **Defend:** The JFPASS will automate the defense actions by centrally managing the deployment of passive defensive measures and by providing the local commander with situational awareness regarding the status of the defensive measures. These measures include, but are not limited to, the recommendation to implement a change in the FP Condition (FPCON), the automatic deployment of barriers and the use of robotics for threat intervention.

5. **Recover:** Although the JFPASS will not directly contribute to the recovery function, the synergistic effect of integration and automation within the other areas of the FP construct will help in resuming effective operations and provide a deterrent against further attacks. (2008, July 21)

H. Operational Benefits

The operational aims of the JFPASS are to integrate, automate, and leverage the benefits of integrated systems for joint force protection. The JFPASS will address this need by integrating C2 Architecture and will include the following, taken from a PowerPoint presentation created by Lama (2007, October 24) which indicates the benefits:

- Standard/scalable connectivity (plug-and-play),
- Common and integrated operational picture,
- Decision support system,
- Reduced workload, and

- Affordable logistics and maintenance.

I. Summary of Chapter II

This chapter discussed the need for the DoD's use of new technology to provide WFs with a better defense against a varied and changing threat. The JFPASS is intended to enhance force protection by providing a base defense security system that can detect, detour, and defeat a wide range of threats, while making efficient use of financial and manpower resources. This chapter outlined the rationale for the JCTD model in general and the JFPASS in particular. Chapter III will explore the envisioned capabilities and uses the JFPASS will provide to the WF.

III. Envisioned Capabilities and Uses

A. Desired Capabilities

JFPASS potentially offers new and desired capabilities to the WF in the FP arena. With the threat of attacks coming from multiple enemies, a robust system is needed to provide better and more accurate information about the threat. The JFPASS aims to do this with the following:

1. Near Real-time/Integrated/Interoperable, Comprehensive Land and Maritime-based Reg balanced Local Force Protection (FP) Systems;
2. Common Operating Picture (COP) tailored to suit the user's information requirements and built from fused sensor and other information sources;
3. Scalable FP area of interest to support a single integrated group (military and civilian);
4. Compliance with regional requirements (e.g., laws, regulations, SOFAs);
5. Suite of systems under a central core, ability to share information (voice data and video) with subordinate units, higher headquarters, and adjacent C2 nodes;
6. Standardized core systems training, common baseline of equipment, interface, and training standards which reduces the total lifecycle cost of ownership and facilitates the plug and play use of components among the services and our coalition partners;
7. Internationally releasable system suite (between partner nations);
8. A decision aide to select a system suite for various applications/environments; and
9. CONOPS and TTPs developed for the employment of the integrated system-of-systems (Guardian Six, 2008, July 11).

B. Interoperability

The JFPASS aims to incorporate comprehensive situational awareness to reduce manning through the use of systems integration and robotics. According to the *JFPASS JCTD MTP*, the system:

> will maximize COTS hardware and software while leveraging existing FP systems. To minimize the impact to legacy interfaces/standards the JFPASS JCTD will apply SEIWG ICD-0100 as the standard communication/data exchange protocol. This approach allows the JFPASS JCTD to minimize changes to communications systems or networks while at the same time maintaining the ability to revert to legacy systems. In addition, this approach provides a systems architecture with no single point of failure and plug and play functionality. (2008, July 21)

While complex in explanation, the physical system is simple. The graphic in Figure 2 depicts the systems nodes and the systems resident at each node to support the JFPASS JCTD operations. It also identifies the interfaces between the systems and the systems' nodes. As illustrated, the core technology of the JFPASS JCTD is the Fusion Automation and Decision Support System (DSS) hub (2008, July 21).

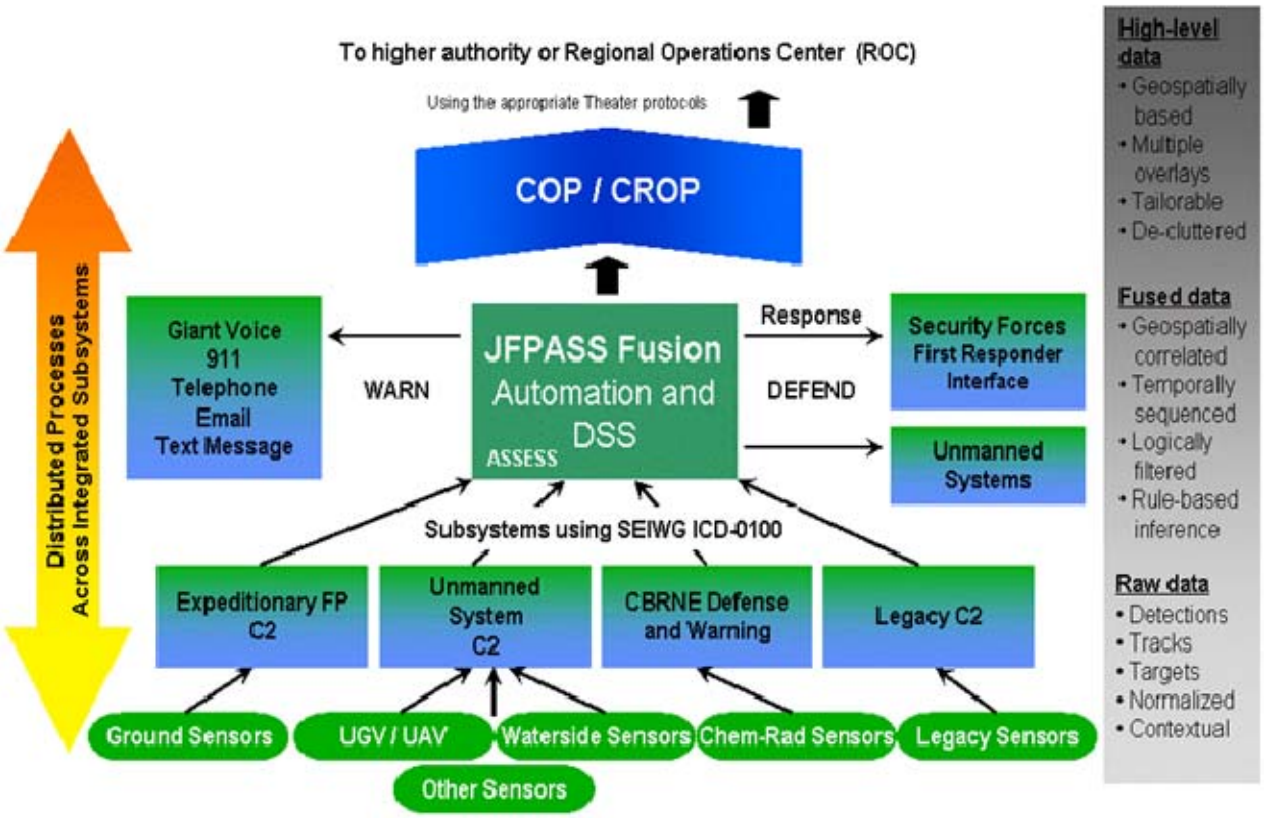


Figure 2. Conceptual Systems View of the JFPASS
(Guidance Six, 2008, July 11)

In order to augment the system, certain external components can enhance detection ability. These include thermal imaging, mobile patrol, and radars. Infrared detectors can be used to help find targets at night or in complete darkness. Such technology could be helpful to combat night attacks.

Mobile patrol sensors, such as unmanned patrol craft, can be used on land, air, or sea. This technology can be mounted on land vehicles, small boats, or aircraft. The US Army has installed a version of this technology on its Mobile Detection Response System (MDARS). This new technology has been successful in detecting intruders out to 300 meters. Finally, surveillance radars

such as SQUIRE can be used to detect moving ground targets. This technology can be used to protect oil fields, bridges, waterways, and other valuable sites.

The aforementioned technologies are further explained by Endress (2007, July), an expert in Security Management:

- Thermal Imaging Technology—objects detection and identification, tracking, surveillance, threat warning, damage assessment, and communications. Examples of this technology are found in optical target designators, radars, laser rangefinders/designators, and vehicle-mounted Infrared Search and Track and Forward-Looking Infrared packages in combination with secure real-time data links and decision and navigation aids;
- Mobile Patrols—same as thermal Imaging Technology but conducted at sea, air, or ground. Examples of mobile patrols are found in naval patrol boats and surveillance aircraft;
- Ground Surveillance Radars—protect airports, industrial processing facilities, power plants, or areas of special interest by detecting terrorist activities and illegal infiltration. Examples of this are the SQUIRE Surveillance radar and the EL/M-2128 Miniature Detection Radar, often referred to as MINDER. (pp. 79-80)

The JFPASS will be utilized to facilitate control of various “off-the-shelf” surveillance systems to protect US military assets, infrastructures, and people from terrorist attacks.

C. Existing Capabilities and Needs

Integrated security systems such as Tactical Automated Security System (TASS) served as the predecessor to the JFPASS. TASS developer Col Russell Peter, USAF stated in an interview conducted by *Air Force News Service* (Heitman, 1998) that the challenge is to develop a force protection system that is integrated with the many other systems already being employed (p. 1). A shift in force protection priorities that Col Peter observed in 1997 was toward the protection of people rather than high-value areas (p. 1). Peter claimed, "In the past, most of the effort has been to protect weapons storage areas or high value areas. […] While that is still important, we are concentrating on the risk to people.

With terrorist activity becoming so common, we have to worry about truck bombs, for instance" (p. 3).

Force protection integration not only includes current weapon systems but also infrastructure such as medical staff, civil engineers, and communication systems. Representatives from some of these areas have deployed abroad to help establish security systems. This move is in sharp contrast to the traditional military security teams who had the exclusive responsibility of setting up the perimeter security system (p. 3).

Increased awareness of what is happening in this “stand-off” area can lead to enhanced force protection. With more threat warning, people and assets can be better protected from terrorists (p. 3). According to Col Peter, a key element to the future of force protection is looking beyond the base perimeter; he stated, “observing what is happening in the ‘stand-off’ area outside of the gate can provide a valuable early warning to impending danger” (p. 2). A system such as the JFPASS can provide additional portable force protection against immediate threats similar to TASS (Carey, 1998, January 1).

The force protection function has been historically dedicated to physical security, but the TASS program has been expanded in order to integrate intelligence functions and provide enhanced detection and assessment of intrusions to designated sites and their perimeter areas (1998, January 1). Col Peter explained:

> Our goal was to develop a security system that would overcome problems—the labor-intensive nature, complex installation, cabling requirements—that traditional security systems posed for segments of the military that required mobility and rapid deployment. A mobile, modular-type security system, one that was wireless, that would work during the dark desert nights, that could be put together and transported on not more than two airplane pallets, and that could be ready to go in the event of an international crisis. (Heitman, 1997, p. 3)

The advance warning or notification, however, was impossible to achieve at that time. In November 1997 (Heitman), Col Peter said, ”Modeling and simulation can show us where the threat zones are, so we know where we need to put more people or sensors”; yet, he added that “no specific systems fill this gap, but by combining things like unmanned aerial vehicles, satellites and other existing technologies, force protection needs can be filled” (p. 2). Peter’s explanation was expanded in a separate article (Carey, 1998, January 1): “Our vision for this new program office is to be a world class leader in applying technology to force protection command and control systems for the safety, security and survivability of US warfighting assets, WFs and dependents worldwide.”

Many of the JFPASS’ specific capabilities already exist. Internal to the Army, funding for a new development program called the Mobile Detection Assessment and Response System (MDARS) is ongoing. This system consists of an autonomous vehicle designed to provide “intrusion detection and inventory assessment” (Tiron, 2004, May). Equipped with various radars for both scanning and navigating, it can be programmed to patrol an area and record anything within radar range. The platform also includes an RFID sensor that can inventory material inside secure storage locations or containers (2004, May).

Other equipment for possible integration includes an HMMWV with a 30-foot radar mast added to the top. Vehicles such as this can be temporarily positioned in strategic locations to provide detailed coverage for a surveillance area.

The Mobil Detection Assessment and Response System (MDARS) is designed to operate with the Army’s future combat systems or other unmanned vehicles with little assistance from the end user. The MDARS can be upgraded with various communication/interrogation packages to fit particular mission needs and particular platforms. Everything from an all-weather surface detection to ballistic and nuclear biological and chemical threat detection may be performed

with this system on an array of different platforms. This could be an important system to expand the JFPASS component capability.

However, the MDARS does not solve the interoperability problem. Adding more equipment to the mission is subject to diminishing marginal returns. Interoperability is the answer, not more equipment.

D. Development of the JFPASS

ViaLogy LLC, a subsidiary of ViaLogy PLC, was chosen by the DoD for joint experiments to develop Joint Forces Protection and Base Security Systems to support the JFPASS JCTD. ViaLogy was selected to provide a command and control (C2) platform for the experiments (London Stock Exchange, 2007, April 30). At a recent integration assessment supporting the JFPASS, two systems—Northrop Grumman's TASS and Joint Battlespace Command and Control Station (JBC2S) for unmanned systems—successfully demonstrated interoperability (2007, April 30). ViaLogy claims that it "has also integrated a Lightweight Chemical Detector (LCD) to validate the 'plug-and-play' capability intended for JFPASS. The LCD is part of the soldiers' hand-held equipment and is used for checking cargo, personnel or buildings for chemical warfare agents" (p. 1).

According to ViaLogy CTO, Dr. Sandeep Gulati, "JFPASS's real-time requirements present an ideal problem set for their Sensor Policy Manager (SPM). The product is designed for scalable implementations involving 100s to 1000s of sensors and video endpoints" (2007, April 30, p. 2). However, due to budgetary pressures and the new JCTD model of streamlining programs, affordability will be essential to the program's viability and success. As indicated by ViaLogy, the need for increased force protection

> will drive procurement of new standards-based commercial-off-the shelf (COTS) products and interoperability solutions. Emerging sensors such as smart electronic fence, intrusion detection radars and video surveillance offer promising solutions for threat detection and rapid response and base operation. However, the challenge of integrating these sensor and threat

> detection systems over a secure network into a highly reliable "system-of-systems" with both lethal and non-lethal response capabilities has also increased significantly. (2007, April 30, p. 2)

Numerous COTS technologies can provide a synergy of support, which will greatly increase the effectiveness of the JFPASS. For example, Delta Scientific SC3000 gates were recently installed at Naval Station Pearl Harbor. Some of the technology employed in these access systems can be used in other perimeter security systems. For example, the SC3000 utilizes an RFID tag placed on authorized vehicles (2007, April 30). Rather than having a sentry grant access, vehicles need only pull within range of the sensor for the gate to recognize the pre-authorized vehicle and grant access. These systems can even employ RFID tags that operate without batteries. Such passive systems reflect the RF signal back to the reader in order to unlock the security device. RFID gate technology could be another valuable piece of a complete JFPASS system. RFID technology can serve as a key component to automating numerous aspects of a total security system. This new technology can be incorporated into the JFPASS Decision Support System (DSS) for future use.

E. The JFPASS Used for Infrastructure

Critical infrastructures are important. The *US Patriot Act* defines critical infrastructure as those "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health, safety, or any combination of those matters" (National Strategy for Homeland Security, 2002, pp. 29-30). Therefore, any terrorist attack aimed at these facilities could cause grave damage to the US economy and to the safety of its citizens.

While not specifically mentioning the JFPASS or the changing enemy threat environment, Christian Endress (2007, July), editor for *Safety and Security International* and a national expert on crisis management, has pointed out

several new technologies designed to secure critical assets against enemy attacks (p. 79). In a recent article (2007, July), Endress observed that the number of "critical infrastructure targets" in Europe alone is staggering (p. 80). If critical infrastructure is taken to be anything that is "critical for economic prosperity"—to include entities with important interactions with other elements—then the number is truly mind-boggling (p. 80). Anything from the water supply to the telecommunications system can be a potential target.

Nations, therefore, have a vested interest in developing security systems that can help protect critical infrastructure. As Endress (2007, July) points out, fully protecting a critical asset may be extremely difficult but setting up a surveillance system to watch over those potential targets is inherently better than not providing any sort of security. Of course, the cost of a surveillance system is a key consideration in acquired levels of protection.

Perimeter security products can be employed as another layer of defense. While observation-based systems may not stop an attack, they provide critical early warning about impending danger.

Numerous countries have focused on methods of protecting critical infrastructure. In the United States, the Department of Homeland Security has identified 17 critical infrastructures and key resources sectors:

- Agriculture and Food
- Banking and Finance
- Chemical Production
- Commercial Facilities
- Communications
- Dams
- Defense Industrial Base

- Emergency Systems
- Energy
- Government Facilities
- Information Technology
- National Monuments and Icons
- Nuclear Reactors, Materials and Waste
- Postal and Shipping
- Public Health and Health Care
- Transportation Systems
- Water (Department of Homeland Security, 2007a

Should these critical infrastructures become damaged, destroyed, or contaminated, this nation's security, economy, public health, safety, or a combination thereof could be jeopardized (2002).

F. Summary of Chapter III

In this chapter, we have discussed the need for increased force protection on and around forward operating bases as well as other primary installations. JFPASS JCTD research and development shows numerous applicable COTS technologies. In order to create a system synergy, a common communication protocol is required to enhance the interoperability of the system-of-systems. The JFPASS is a JCTD that can make an immediate impact. In short, this technology network can provide the capability to meet the changing enemy threat with current technology.

IV. Defining the JFPASS

A. Introduction

A commander's need for accurate and timely information in support of complex decisions requires that application programs, intelligent agents and humans be able to exchange, analyze, interpret and report information. While interoperability of soldiers has traditionally been accomplished through the creation of tacit and explicit knowledge through training, construction of software applications and intelligent agents for training programs, the evolution of technology requires a standardized vocabulary and semantically rich formalization of common-sense knowledge for the various domains of operation spanned by military planning and operations. This formalization is appropriately captured in ontologies (specifications of conceptualizations) that provide representation vocabularies and facilitates information exchange (Burk et al., 2007).

This chapter provides a detailed description of the JFPASS, which provides the information of value added. In Chapters II and III, the process in which the JFPASS would provide the WF with an advantage was described by explaining how FP would be increased and which systems would be used. The JFPASS would interface current FP systems that would, in turn, increase the interoperability of COTS and decrease an enemy threat.

Interoperability has always been a primary objective of any program within the DoD development and acquisition process. However, recently this concept has been expanded to include the application of what maturing technology can provide the military and what the JFPASS can provide the WF, which is volumes of data and pertinent intelligent information. First, we must define four key words that are the baseline for understanding the JFPASS. They are as follows, outlined in the IAP for the JFPASS JCTD (United States Army, 2008, October 14):

Automation: Combining data points to automatically perform a task otherwise done by an operator.

Integration: As defined in the JFPASS JCTD, there are two aspects that determine full integration. First, the fundamental aspect of "technical" integration is the baseline requirement for a system/technology to work within the digital architecture of the JCTD utilizing ICD-0100b. Second, the integrated component must be fully controllable from any BC station or operator station.

Interoperability: Joint Publication 1-02 defines interoperability as "1. The ability to operate in synergy in the execution of assigned tasks. 2. The condition achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them and/or their users."

Fusion: Fusion may be defined as a series of processes performed to transform observational data into more detailed and refined information, knowledge, and understanding.

Additionally, intelligence and context are key contributors to the JFPASS.

B. What Does "Intelligence" Mean to the JFPASS?

How do researchers talk about intelligence in the context of a machine? Some could argue that even though a computer is able to store vast amounts of data and is capable of processing millions of computations per second, it is nevertheless only a machine that is entirely restricted to following predefined instructions (Pohl, 2004). Based on this perception, it is important to briefly discuss the concept of intelligence and the sense in which this perception is applied to computer software (2004).

Intelligence within a machine differs from a human's path toward a new idea or solution to an existing problem. Both use pre-existing relationships to analyze and produce a logical solution. Machines are restricted by the limitations

of the human and the human is restricted by experience and education. Some might argue that machines are bound only by their predefined instructions. The same argument applies, in a sense, to humans—growth and education determine the ability to discover the means to understand empirical data. By comparison, computers, despite their restrictions, can evolve much faster than humans can. Where humans take generations for evolution to occur in their intellectual abilities, well-designed computers revolutionize capabilities within years. These abilities greatly differ due to the advancements in technology over the last twenty years.

In his paper, Dr. Pohl states:

> Webster's Dictionary defines intelligence as the '…capacity for learning, reasoning, and understanding." This definition suggests that there are component capabilities that contribute to the concept of intelligence. Further, these component capabilities are not necessarily powerful. In other words, it may be argued that there are levels of intelligence and that at the lowest level such capabilities must include at least the ability to remember. Higher levels of intelligence include reasoning, learning, discovering, and creating. Certainly at least some of these intelligent capabilities can be embedded in computer software. (2004)

Intelligent software has the ability to create relations needed by building an ontology with all pre-existing systems, thus providing support to the growing demand for information that is accurate, timely and high quality. However, the information is only as good as the context it is provided.

C. Why is Context Important in Defining the JFPASS?

A current myth is that computers are the backbone of the Information Age because they can store and process vast amounts of data. However, we must remember that the only purpose for storing data is for later use (Pohl, 2004). DoD's computer-based systems do not automatically analyze data; they require human interaction to interpret the data provided. Derived data or "context" is the key ingredient that is missing (Pohl, 2008, October 21). Context is the interpretation of data by the user in a logical and applicable way (Pohl, 2008,

October 21). The JFPASS must answer one important question: Can software provide valuable and pertinent information with COAs in order to respond to the threat inferred from the intelligence gathered? Basically, the JFPASS must provide intelligent information on its own to the WF with no interaction from the WF.

D. Data-centric Environment

1. Current Situation and the Need for Intelligent Software

Technology has revolutionized the way the world views force protection. The advent of intelligent software has given force protection technology the ability to interpret and answer questions. The need for intelligent software to discard irrelevant information and analyze only relevant data is key to timely, accurate and useful information for decision-making by the WF.

There are two primary reasons for software to incorporate intelligent software capabilities. The first is to reduce the current bottleneck in the data processing stream. Over the past 20 years, electronic data storage capabilities have greatly increased the availability of timely and relevant information, but they have (paradoxically perhaps) increased the time needed to take action. This problem is due to the historic belief that it is the user's responsibility to interpret the data into information and knowledge, aided by the computer-based system. In the past, computer systems were designed to store and retrive data, while any manipulation was conducted by the users. This does not, however, provide useful information in a context similar to the question or problem initially posed. Can the JFPASS provide pertinent intelligent information? The second reason is financial. The growing complexity of communication and network systems and the increasing reliance of organizations on technology information systems require research and development of intelligent software for their existence and profitability (Pohl, 2004).

2. Transition from Data to Information by Intelligent Software

The interoperability of information systems is an important issue for many organizations. It is a major concern for integrating systems both within and across organizations, and, in the case of this paper, across the military branches. The key deliverable is the movement from data collection and processing to providing intelligent information from data. Within the military, the planning process occurs concurrently at multiple echelons in a highly distributed environment, which are seriously impeded by:

- An overwhelming volume of data,
- Scarce timely and actionable information,
- Poor vertical and horizontal communication,
- Uncertainty with respect to the reliability, accuracy and completeness of information, and
- Limited ability to rapidly determine the overall, current state of the planning process. (Pohl, 2004)

This results in time delays, conflicting planning efforts, confusion, wasteful use of human resources, and missed opportunities (Pohl, 2004). This is due to the absence of context within the computer systems. The user must interpret and manipulate data by adding context. Unorganized data has low value and is usually copious. As movement occurs vertically, we see data increasing in value and decreasing in volume. This is due to the elimination of data that provides no added value to the specific question of the problem being addressed.

The JFPASS attempts to provide context in which information can be derived from data. This would be done by integrating COTS systems to build a package with significant value to the user. The JFPASS can infer context from principal components defined by the user. These components are location, time, history, urgency, activity, culture, identity, and environment. If fully successful, the JFPASS will be able to automatically gather, process, and interpret pertinent data within a user-defined context and can provide COAs to the user.

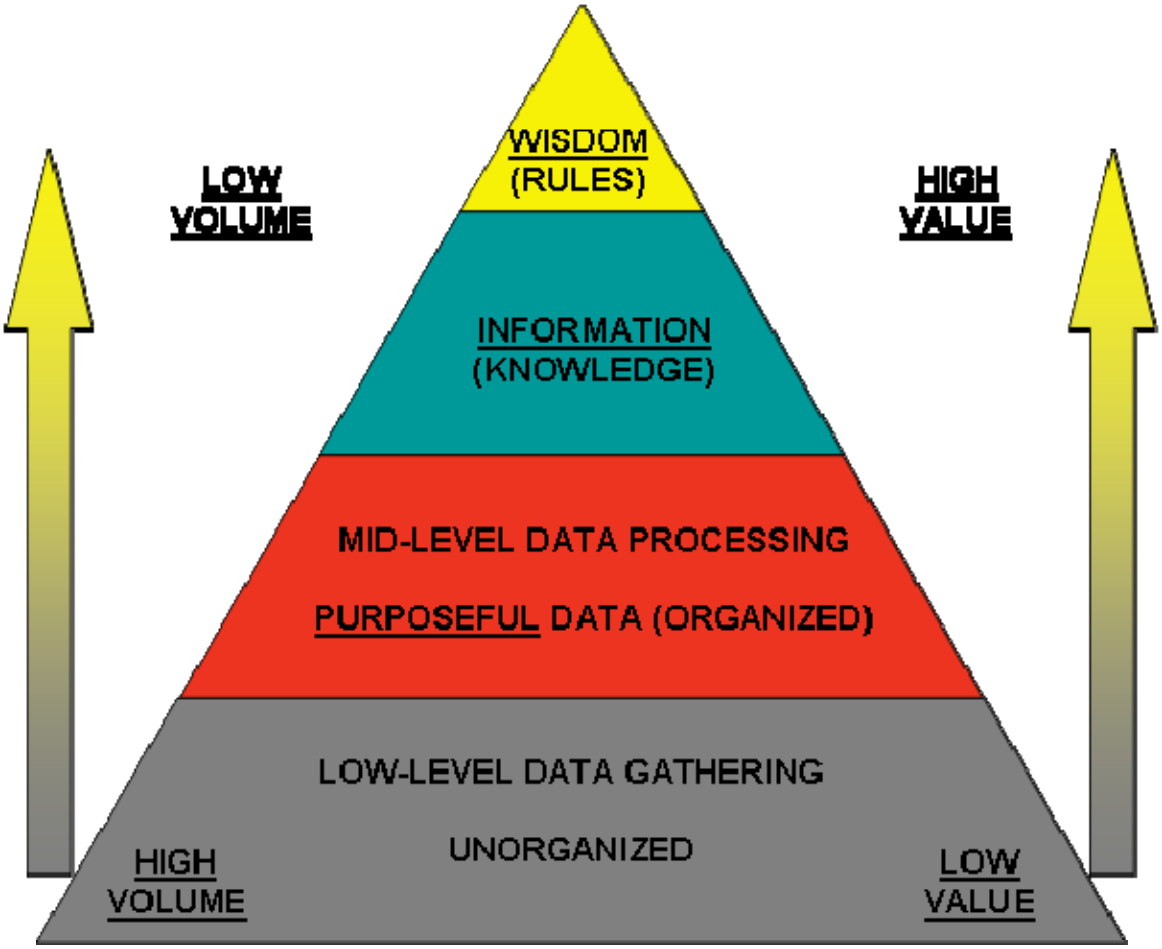


Figure 3. Transition from Data to Knowledge
(Pohl, 2005)

The vertical flow depicted in Figure 3 assists in understanding the relationship between the user and the computer. By adding context to data, information can be obtained for decision-making. Information becomes knowledge, which allows the WF to build upon the low-level data for the institution and creation of rules. There are distinct differences between human and computer analysis of data. Although computer information is defined by the parameters set forth by the WF/user, the computer has distinct advantages over the human approach to analysis as seen in Tables 1 and 2.

Table 1. Advantages of Human Simulation

Flexibility	Use is not constrained by the parameters of the designer/user
Reliability	Perhaps not compared to a mature system but certainly an issue for an experimental system
Responsiveness	Production can be faster but quality will suffer
Ease of use	Learning the interface and procedures are simpler

Table 2. Advantages of Computer Simulation

Applicability	Feasible to simulation more complicated and longer sections of COA
Reproducibility	Can return to a situation for re-examination
Traceability	Traces decisions back to results and results back to data and data sources
Speed	Runs much faster than real-time, and multiple runs
Accuracy	Learning the interface and procedures are simpler

Regardless of strengths, no information provided by the computer will be used to support decision-making unless it also approaches the advantages of the human analysis, especially if the intelligent information provided by the software is credible and useful to the WF.

E. Ontology of Intelligent Software

Ontology is similar to a dictionary or glossary but with greater detail and structure that enables computers to process its data. Ontology consists of concepts, axioms, and relationships that describe a domain of interest. That is, ontology is a description (like a formal specification of a program) of the concepts and relationships that exists for an agent or a community of agents (Gruber, 1995, November). Loosely translated, ontology is the entire knowledge in a particular field. Ontologies are designed to share knowledge with and among agents in a defined field. The JFPASS agents are the COTS components that will provide the information to the WF.

Recent work in Artificial Intelligence (AI) is exploring the use of formal ontologies as a way of specifying content-specific agreements for the sharing and reuse of knowledge among software entities. By creating these agreements, multiple systems can provide relative and pertinent information for the user to make decisions.

We use common ontologies to describe *ontological commitments* for a set of agents so that they can communicate about a domain of discourse without necessarily operating on a globally shared theory (Gruber, 1995, November). As researchers, we say that an agent *commits* to an ontology if its observable actions are consistent with the definitions within the ontology. The idea of ontological commitments is based on the Knowledge-level perspective (Gruber, 1995, November). However, the user or designer creates the definitions within the ontology, thus the human interface still exists.

The Knowledge Level is a description of an agent's knowledge that is independent of the symbolic representation used internally. Knowledge is attributed to agents by observing their actions; an agent "knows" something if it acts *as if* it had the information and is acting rationally to achieve its goals. The "actions" of agents—including knowledge-based servers and knowledge-based systems—can be seen through a tell and ask functional interface, where a client

interacts with an agent by making logical assertions (tell) and posing queries (ask) (Gruber, 1995, November).

F. Risk

Typically, risk management has focused on only single systems, and often only on development risks. For Systems of Systems , the approach has to reach beyond these boundaries and across the lifecycle from before acquisition to operations, sustainment, and retirement. A venture as important and as complex as creating a system-of-systems to provide increased FP involves many types of risk. Both the development and testing efforts will be discussed along with the identification of some potential tools to mitigate those risks.

Figure 4 shows a basic risk management process that can be used to monitor and mitigate risk during the development and testing of any program. Implementation of this model can assist in elimination of waste.

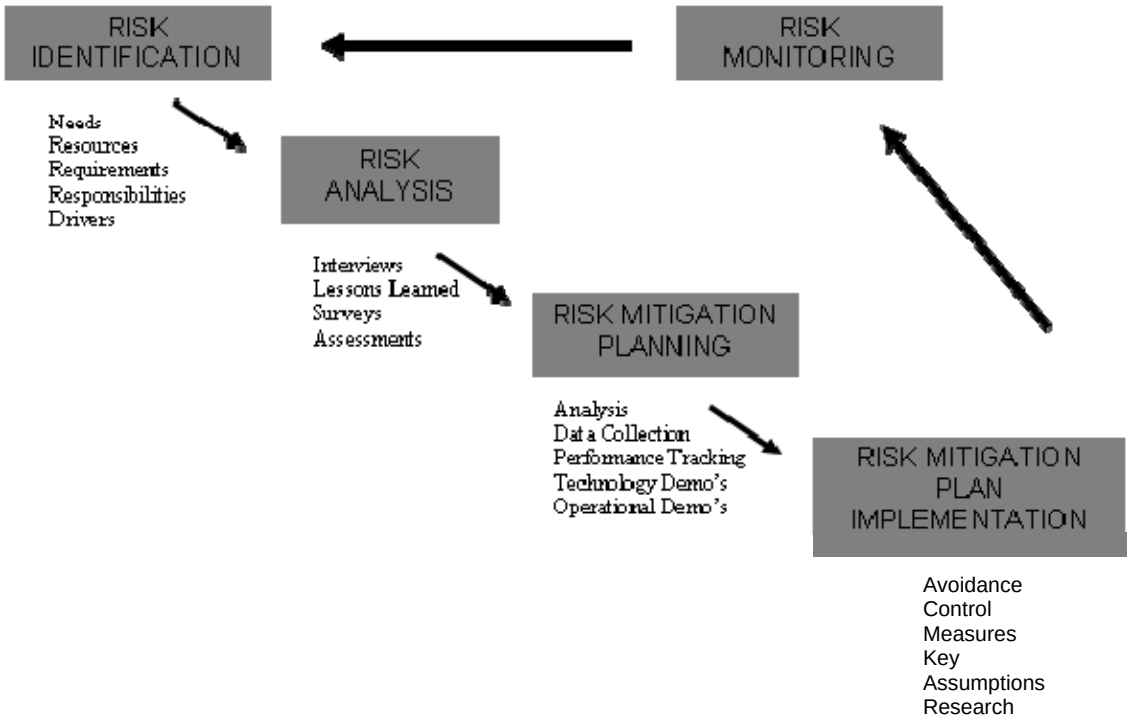


Figure 4. Basic Risk Management Process Model

However, the complexity of the JFPASS will require considerations beyond those of the typical risk management model. Considerations that should be addressed are as follows.

1. Considerations for Systems of Systems

Risk management is a good starting point for reviewing how acquisition processes deal with Systems of Systems (SoS). Risk analysis is typically an early step in an acquisition and for an SoS, that risk analysis is an especially critical step. For an SoS, or for the more likely case of a system or component that participates in an existing SoS, an effective risk management approach should do the following:

- scale to size and complexity of Systems of Systems ,
- incorporate dynamics,
- integrate across full lifecycle from requirements to sustainment, and
- focus on success as well as failure. (Creel, 2008, June 5)

2. Scale to Size and Complexity of Systems of Systems

Most traditional risk management methods cannot address the complexity that arises when multiple systems are routinely combined. State-of-the-practice risk management approaches provide stakeholders with a long list of potential problems (in the form of risks). The list for a single project, program, or technology often includes more than 100 statements of risk. For Systems of Systems , that list of potential problems can be overwhelming (Creel, 2008, June 5).

Table 3. Common Systems of Systems Risk Management Issues
(Conrow, 2005, February)

Number	Issue	Issue Summary
1	Multiple Stakeholders	Differences in stakeholder's behaviors will often lead to contention and potentially sub-optimal design solutions, funding allocation, schedule priority, and increased risk.
2	Multiple Risk Management Processes	Differences in risk management processes and their implementation can lead to the omission of risks as well as exaggeration of other risks.
3	Long Lifecycles	Non-uniform acquisition maturity potentially complicates risk management.
4	Common Technical Risk Causes	Technical risks are often examined, evaluated, and managed separately, which may not provide insight into weaknesses/shortfalls.
5	Integration Risk	Integration risk is often not explicitly evaluated. (In the case of the JFPASS, this risk would be detrimental if ignored.)
6	Functional Performance Risk	Functional performance risk is often not explicitly evaluated.
7	Interface Complexity	It is generally difficult to evaluate interface complexity and accurately relate it to risk.

The JFPASS must also consider risks associated with existing programs of record. DoD acquisition programs already run the gamut from relatively simple to very complex. Complex hardware and software interfaces often exist within individual programs, as well as in SoSs. While there may be a desire to explicitly treat complexity in a risk analysis, it is generally difficult to accurately relate complexity to risk. Furthermore, efforts to estimate the risk of interface complexity directly may lead to uncertain, subjective, and/or erroneous results (Conrow, 2005, February).

The JFPASS must also consider the required support for technologies under consideration. The primary key in reducing risk is effective communication between all those involved.

G. Summary of Chapter IV

Converting the vast amounts of raw data into comprehensive, actionable data is truly what the WF needs from an FP system. Soldiers can process this information themselves and make intelligent decisions but often this is not the most efficient use of a limited resource. This is where the JFPASS seeks to provide aide to the WF. By compiling vast amounts of data and intelligently processing it, the JFPASS promises to deliver information to actually support operational decisions. A degree of trust (and, therefore, a level of risk) accompanies the WF's reliance on a machine to help make decisions in life-or-death situations. This risk is offset by the reward of enhanced information-processing power. By leveraging the JFPASS technologies, more information can be processed in a shorter amount of time—yielding more accurate information about the threat. The WF's task load is then greatly reduced, which allows soldiers to concentrate their attention on higher order processes.

V. Results

A. Introduction

This chapter provides a framework, description, discussion and analysis of some issues and factors that must be considered in constructing a new FP system in response to the following: How does the use of force protection equipment contained in the JFPASS impact force effectiveness?

Based on preliminary results of the background research (Chapter III), the JFPASS plans to create a "fusion cell" concept to control COTS implemented with a common communications suite of protocols to provide a common use language. Because of the diverse and complex nature of work to be performed, the JFPASS will need to craft a strategy that integrates these diverse elements in order to meet user requirements. A detailed discussion will address how and why specific data was collected by the project team to answer the question previously stated. Through the means of a survey, interviews and literature research, we obtained an answer.

It is important to note that the strategy discussion and the analysis below do not capture all the issues that must be considered prior to program recommendation to OSD. However, they outline considerations that require attention and possible solutions, including the WF's view of the JFPASS.

B. Demonstration Strategy

The JFPASS JCTD Demonstration Strategy will consist of both Technical and Operational demonstrations. It will conduct two sets of demonstrations:

1. Technical Demonstration One (TD-1) will demonstrate the full suite of JFPASS JCTD capabilities in preparation for a limited utility assessment.

2. Technical Demonstration Two (TD-2) will be a preparation for the Spangdahlem site-specific Operational Demonstration 2 (OD-

2)/Operational Utility Assessment (OUA). The Operational Problem, Desired Capabilities, CONOPS and TTP drive each demonstration. (Guardian Six, 2008, July 11)

Table 4 depicts the location for each event.

Table 4. JFPASS JCTD Schedule
(Guardian Six, 2008, July 21)

EVENT	LOCATION
Technical Demo 1	Eglin AFB, C3
Operational Demo 1	Eglin AFB, C3
Technical Demo 2	Spangdahlem AB
Operational Demo 2	Spangdahlem AB
Interim Capability through Extended Use	Spangdahlem AB

Technical demonstrations will serve as technical checks and dress rehearsals before each operational demonstration (OD). A period of evaluation and internal assessment will follow TD-1 to provide the technical team with the information and time necessary to complete preparations for OD-1. OD-1 will serve to highlight the flexibility and scalability of the JFPASS JCTD system. The operational team will execute OD-1; this event provides a Limited Operational Utility Assessment (LOUA) of the full suite of sensor interfaces, data fusion, integration and automation in semi-fixed/expeditionary, and waterside environments. OD-1 may enable early transition of capabilities to the WF's, pending a successful LOUA. TD-2 will serve as the final dress rehearsal in preparation for OD-2 and will provide a final Operational Utility Assessment (OUA) and report of the JFPASS JCTD capabilities (Guardian Six, 2008, July 11).

C. Operational View

Conducting the TDs and ODs will provide opportunities for the end users to observe and participate in the assessment. They will provide instant feedback on the results. The TDs and ODs will provide an operational view of how the JFPASS will integrate the system-of-systems approach and how it will increase the FP capabilities.

The operational view (OV), in Figure 5 below, provides a high-level illustration of the JFPASS JCTD in its operational environment. "It depicts the operational elements nodes and systems information exchange paths. This view serves to support the development of Systems Architecture. It also illustratively describes the CONOPS and supports the development of further CONOPS and TTPs" (Guardian Six, 2008, July 11).

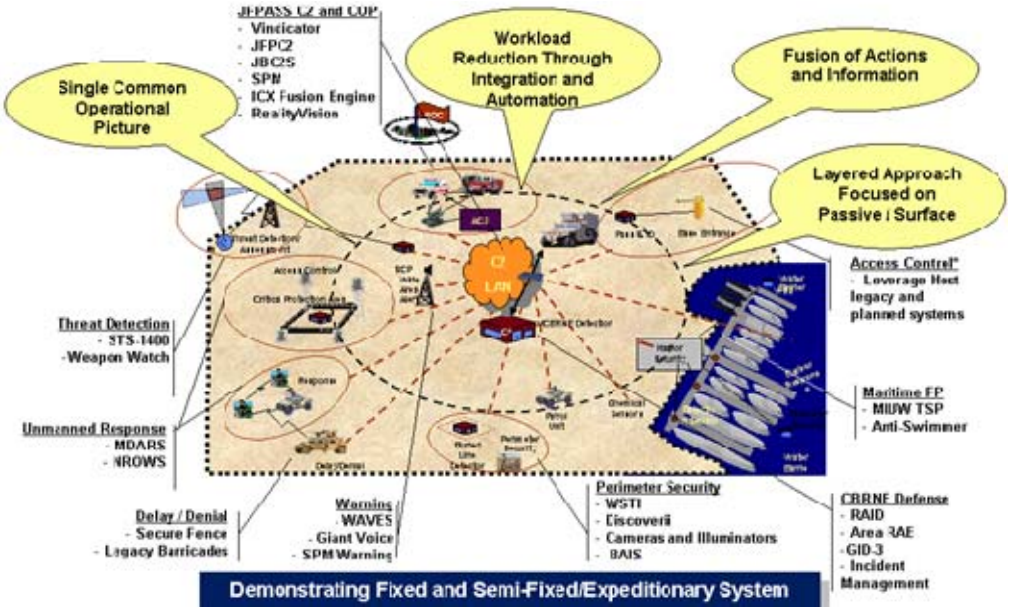


Figure 5. Operational View of the JFPASS
(Guardian Six, 2008, July 11)

The researchers would like to note, however, that the operational view above assumes theoretical interoperability with zero faults in an ideal battlefield. As we know, nothing is perfect and the ability to adapt is crucial to success. The key will be to provide the JFPASS with the ability to adapt to an ever-changing battlefield and an evolving enemy threat.

D. Analysis

1. Importance (Scope)

In our collection of data, the primary questions concerned the need for the JFPASS. As stated in Chapters II and III, the JFPASS will provide the WF with a means to increase FP, both in deployed and garrison environments. However, the need for the JFPASS could not be easily ascertained from current data due to the JFPASS initiative's early stages of development. To date, only one TD had been conducted, with data needed for a comprehensive CBA, which has not yet been available. Taking this into account, we decided to focus on effectiveness. This involved directly polling the WFs (and all those involved with the JFPASS) to assess the level of importance of the desired operational capabilities to overall mission success.

2. Collection

With the creation and utilization of an operational utility assessment model, using a survey featuring direct communication with the operator's experience gave the best source of data. Doing so provided control measures already established by the contractor in charge of developing the JFPASS.

Incorporating a table showing the relationship between key tasks and desired capabilities allowed the importance of the JFPASS to be answered by the WF, as seen in Figure 6. In doing so, control measures already established by the contractor in charge of developing the JFPASS were provided.

By incorporating a table (Table 5) showing the relationship between key tasks and desired capabilities, we are able to demonstrate the importance of the JFPASS according to the WF.

•

	Near Real Time / Integrated / Interoperable, Comprehensive Land and Maritime-based Reg balanced Local Force Protection (FP) Systems	Scalable FP area of interest to support a single mutually supportive group (military and civilian)	Compliance with regional requirements (e.g. laws, regulations, SOFAs)	Suite of systems under a central core	Standardized core systems training	Internationally releasable system suite (between partner nations)	A decision aide to select a system suite for various applications / environments	CONOPS and TTPs
DETECT								
ASSESS								
WARN								
DEFEND								
RECOVER								

Figure 6. Mapping Tasks to Capabilities
(Guardian Six, 2008, July 11)

The levels of importance were crucial in answering the level of mission success that the JFPASS would have from the WF's perspective. In Appendix A, the levels of mission success in relation to each of the five key tasks and eight desired capabilities are explained. The following analysis represents a sample size of 39 operationally experienced WF's deployed within the last 24 months. Their survey responses can be seen in Appendix D.

3. Quantitative Analysis Method

a. Data Interpretation

In order to derive quantitative results from the survey distributed, we wanted to analyze the trend of scores for each desired operational capability (x) as compared with the five standard key tasks (y) outlined by the lead agency of the program. Upon reviewing the relative scores of the desired operational capabilities, we realized that some further insight could be derived from analyzing the standard deviation of these scores to verify what areas most consistently concerned the raters.

b. Data Analysis

We first averaged all survey respondent scores in each category and then averaged all categories. We forced the averages in each category to a mean of 3.0. This was accomplished by taking the difference between the overall average and 3.0 and then subtracting that value from the value in each category. This effectively smoothed our results by preventing numerous low scores in a category from artificially accentuating a single high score. Consistent raters, therefore, would show the same relative weights as raters with a much greater range of scores.

Upon graphing these forced mean scores against their individual key tasks, we began to see a trend depicting which operational traits were most important and in which areas their importance was most significant, (see Appendix E).

We wanted to verify that a few high scores were not the cause of these inflated averages. To determine this, we graphed the standard deviation of all survey scores by individual desired operational capabilities. By graphing these results in a polar graph, we saw a relative depiction of the amount of variation in the desired operational capabilities scores according to the performance parameters that our surveys rated against. The final result can be seen in how tight the "shot group" is on the target of zero variation (see Appendix F).

After building our WF preference analysis, we created a model to compute an overall measure of effectiveness. By defining a field to be filled in once test data becomes available, we were able to build a formula from the product of the individual capabilities multiplied by the sum of the operational preferences across all five standard tasks. We then summed each product to produce one measure of effectiveness score (see Appendix G).

The overall measure of effectiveness was then plotted on a polar graph with each functional area represented on a separate spoke, as seen in Figure 7.

Figure 7. Overall Measure of Effectiveness Shown as a Representation of Means Dispersion in a Polar Format

By graphically plotting the products of the test plan results with operational preferences, we have shown an effectiveness dispersion of capabilities. This graph can be used to focus performance development to match WF preferences.

4. Quantitative Results

a. Measuring the Results

Several interesting trends surfaced as a result of analyzing the survey responses. The desired operational capabilities all had a relatively similar level of preference from the surveyed WF's. This shows that the functional areas chosen to survey represent a well-balanced group of emphasis. However, several distinct trends emerged from our survey. For example, near real-time information was clearly the most important factor for our respondents. Given the high preference score for near real time information, as seen in Appendix D, it is particularly interesting then that this desired operational capability had the lowest standard deviation of survey responses across all the desired operational capabilities—leading to the intuitive assumption that knowing what and where the threat is occurring leads to greater mission success. A sample survey from Appendix D is shown below:

1	Near Real Time	Scalable	SOFA Compliant	Suite of Systems Central Core	Standardized Training	Internationally Releasable	Decision Aide	CONOPS and TTPs
DETECT	5	4	3	5	2	3	3	2
ASSESS	5	4	4	2	5	3	4	4
WARN	5	5	2	2	3	1	3	1
DEFEND	5	1	3	4	2	5	5	3
RECOVER	5	3	3	2	2	4	2	1

Figure 8. Sample Survey Format

All eight desired capabilities were measured using the same personal preference assessment. The results were then placed in the aforementioned formula.

b. Interpreting Results

The scores in the near real-time category across all key tasks averaged 46% higher than the scores for the other desired operational capabilities, suggesting that timely information is the most important of these traits to the WF for mission success; see Appendix B for graphical representation and Appendix H for calculations.

In particular, the detection key task had the single lowest deviation, scoring 78% less than the average response. Numbers like these show a clear WF judgment that near real-time information during the detection phase of an engagement is the most important component of force protection (see Appendix H).

The key task of recovery received the lowest scores across all desired operational capabilities, 23% less than the average evaluation score. This shows that the final phase of force protection is the least critical to the WF when it comes to engaging and eliminating a force protection threat. However, given the

constrained resources within the FP arena, the interoperability of the Systems of Systems approach that the JFPASS will provide will lead to a level of increased security and protection.

E. Progress and Change

As mentioned earlier, many of the issues concerning the JFPASS will be better understood only with the completion of the TDs and ODs. Changes are sure to occur after each TD, driving a change in the timing and outline of the follow on ODs.

As seen in this chapter, the effectiveness of the JFPASS depends on the accurate interpretation of the WF's needs. The quality of the JFPASS will ultimately be measured by the relevance of its accuracy and timeliness.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. Discussion

A. Conclusions

1. The Need for Better Force Protection Capabilities

The JFPASS seems to provide much needed advantages in increasing security and decreasing the risk of losing lives, equipment, and infrastructure. This analysis provides insights about what is most important to the warfighter (WF). With the JFPASS, legacy systems can be interfaced with Commercial-off-the-shelf (COTS) and Force Protection (FP) systems to enable reallocation of manpower and reduction of the logistics footprint required to support.

New systems, no matter how safe, have a learning curve associated with their operation and inherently have some risks. The JFPASS seeks to mitigate these risks by tying existing systems together to create a network that can provide intelligent information for better decisions. In this manner, the JFPASS avoids the learning curve dangers of other FP systems in early operations. Whatever the case may be, lack of manning, training, and experience sometimes causes FP systems to be discarded in favor of traditional, labor-intensive FP measures such as manning the watch tower. With limited resources, FP must be given the tools and methodology to work as efficiently as possible; the JFPASS aims to provide this capability.

2. The Way to Fill the Need of the WF with the JFPASS

The JFPASS, if successfully tested and fielded, can be tailored as needed by the WF. Creating a system that fuses numerous FP systems to one location expands situational awareness. This provides the WF more accurate and pertinent information that can support decisions to effectively counter the threat. The JFPASS provides this ability with compact, portable, modular, and fast assembly kits that can be packaged in any form to meet the WF's needs. This allows the needed FP to be brought with a deploying unit or interfaced with

existing FP systems on ground. The result of structuring the JFPASS this way is numerous savings. Reduction in logistic footprint, reduction of transportation costs, minimal manning for installation, and reallocation of manpower are only a few that are immediately impacted by the JFPASS capability.

B. Recommendations

1. What are the *Need*s that are the Focus of the JFPASS from the WF's Perspective?

Accurate, real time information is important. This is especially true in the detection phase. Any WF will say that they can defeat the enemy if they know when and where the enemy will be and where they are planning to attack. However, we know that this information is hardly ever available in a timely manner. Many times the enemy will have the advantage due to an inability to detect the threat. Thus, in the FP arena, reaction to the threat is typically the norm. Anticipating the threat, as opposed to repelling an attack, is the basic capability the JFPASS aims to provide. The ability to gain the initiative will allow the WF to position assets to counter the threat prior to the engagement.

Recovery, though a necessary step in the FP process, is the least important phase. The WF is willing to restrict the usage of limited resources in this area as it is the most removed from the detection phase.

2. Work to Mitigate the Risks Associated with the JFPASS

Given the risk associated with a new system, any work done to reduce that risk will pay significant dividends. For example, redundancies in communication or processing will reduce the risk of losing connectivity. Also, storing of data frequently and providing backup power supplies will reduce the risk of the consequence of service interruptions (e.g., through primary power failure). As mentioned previously, with human life at stake, the inherent risk threshold is low and one of the most significant detractors from accepting the JFPASS as a viable FP system.

C. Payoff

The JFPASS supports the GWOT by providing commanders on the ground and our joint and coalition partners with a Near Real Time, Integrated/ Interoperable, Comprehensive Land and Maritime-based Regional and Local Force Protection Systems to counter threats. This is a precedent-setting solution, using intelligent technology to work more effectively for the WF. It provides the integration of CBRNE and physical security systems through the application of an integrated C2 Architecture that uses computer software and tailored decision-making rules. The JFPASS provides actionable information and allows the user to focus on the response function more quickly and with better accuracy. Currently, no other program is capable of integrating the existing COTS components and fusing them with service-acquired systems into a single, integrated FP system-of-systems. The JFPASS will enhance FP by using intelligent information in an expedited manner, allowing the WF to focus on orchestrating the response. It also provides the opportunity for future cost savings through standardization and the reallocation of manpower.

D. What is Next for the JFPASS

Due to the lack of test and cost data, a thorough BCA cannot be supported at this time. As seen in Figure 9, the BCA is broken into two specific areas: cost and operational effectiveness (a score). Our group focused on the operational effectiveness portion due to the absence of cost data. A full comparison of effectiveness versus cost is required to complete the BCA as illustrated in the figure below.

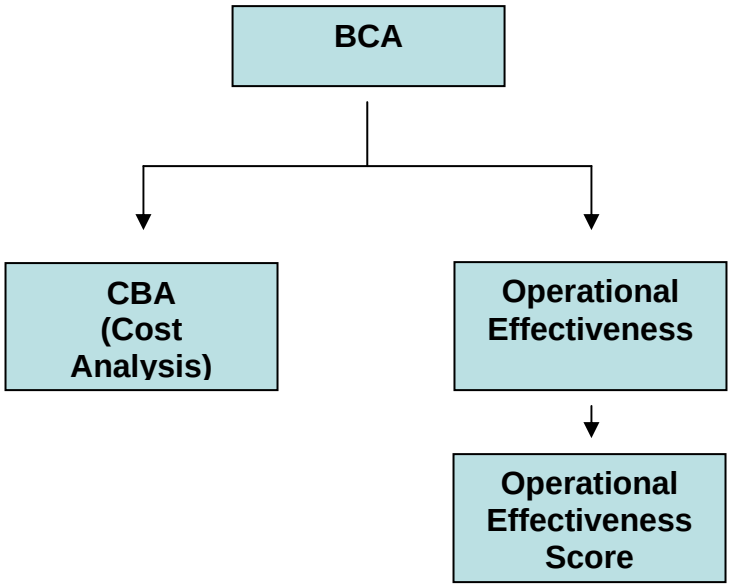


Figure 9. BCA Diagram

As test data becomes available, it will be assessed and fed into the operational effectiveness model to provide an operational effectiveness score. Having this score, formulated from operational experts' judgments of battlefield priorities, will allow cost data to be compared in order to analyze different aspects of what can be eliminated, reallocated, or reduced in terms of FP. Comparison of effectiveness versus manpower costs can be measured to find out where or if reallocation or reduction is a viable option and how much cost savings may be realized. The direct impact of five men versus two men is significant and could be measured using the model represented in this project once test data becomes available.

Figure 10 represents the flow process in which data will travel once testing is done and acquired for input. The new data will be collected, assessed, and fed into the matrix. An effectiveness score is produced based on how operational experts interpret the key tasks mapped against the desired operational capabilities. The operational effectiveness score calculated then provides a useful tool on which to base future decisions. For example, the score will help determine areas where the JFPASS team should focus improvement

efforts, or it may provide a means to compare similar systems to the JFAPSS. The system is currently under testing, but once the tests are completed, the results tabulated, and the data analyzed, then the data could be used to revisit this analysis and update the effectiveness score of the JFPASS.

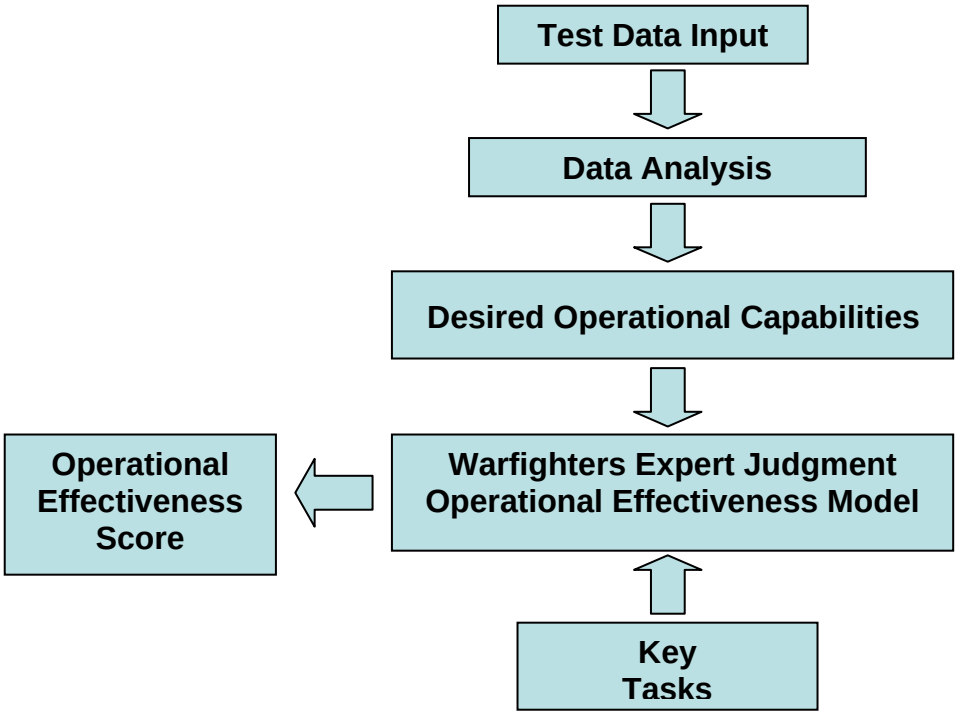


Figure 10. Operational Effectiveness Score Flow Chart

Despite the lack of test data, we conclude that JFPASS has shown clear potential to be a highly effective system for providing modernized and enhanced FP systems with the ability to meet ever-changing future threats.

E. Future Research

It is the authors' recommendation that this work be added to the body of experience and knowledge of the JFPASS JCTD program in order to aid in further development research efforts—not only for the JFPASS but for other intelligent software exploratory programs as well. Specifically, future research

might investigate why the WF's place such emphasis on the need for real-time information. Perhaps more insight may be gained into the nature of FP by clearly understanding how the WF intends to use near real-time information for operational mission enhancement.

Additionally, further research could help to answer why the WF's responses indicated a general lack of concern for the recovery phase. Perhaps incoming threats are so sporadic that quickly resetting the force is not as much of a priority as originally thought. This could then lead to a more accurately tuned system that is specifically geared to react quickly to an initial threat, even at the cost of recovery time. Multiple attacks could occur, however, so the recovery phase must not be ignored.

We conclude by noting that there is a great deal more research that can be done on the JFPASS to assist in assessing its potential. Additional methodologies and/or tools can help managers solve the technical and engineering challenges that are sure to arise with interfacing COTS systems with new software. As with any new program, there are seldom any standard answers; however, there are opportunities to learn from the data and to gain value-added experience from programs such as the JFPASS.

List of References

Ankolekar, A., Seo, Y., & Sycara, K. (2003, August). Investigating semantic knowledge for text learning. In *Proceedings of ACM SIGIR Workshop on Semantic Web*. ACM Press.

Army announces details of FY 2006-2007 budget. (2005, February 7). *US Fed News Service, Including US State News*. Retrieved September 10, 2008, from http://proquest.umi.com/pqdweb?did=1257775451&Fmt=7&clientId=65345&RQT=309&VName=PQD

Auerswald, P., Branscomb, L., La Porte, T., & Michel-Kerjan, E. (2005). The challenge of protecting critical infrastructure. *Issues in Science and Technology*, *22*(1), 77-83.

BAE systems to provide precise threat ID to U.S. Army. (2006). *Military Technology*, *30*(12), 118-127. Retrieved September 10, 2008, from http://proquest.umi.com/pqdweb ?did= 1216892751&Fmt=7&clientId= 65345&RQT=309&VName=PQD

Boehm, B., Boehm, L., & Boehm, J.A. (2007*).* Using the incremental commitment model to achieve successful system development (USC-CSSE-2007-710). Los Angeles, CA: Center for Systems and Software Engineering, University of Southern California.

Bonsignore, L. (2007). Physical safety of armed forces has top priority. *NATO's Nations and Partners for Peace*, (1), 144.

Brown, G., Carlyle, M., Salmeron, J., & Wood, K. (2006). Defending critical infrastructure. *Interfaces*, *36*(6), 530-544.

Burgess, G. (2003). Intelligent software agents for military operations planning. *SimTecT*. Retrieved October 24, 2008, from http://hdl.handle.net/1947/2364

Burk, R., Goerger, N., Gates, B., Blais, C., Nagle, J., & Goerger, S., (2007). Knowledge representation for military mobility decision-making by humans and intelligent software: The mobility common operational picture data model and ontology. *Extending the Horizons: Advances in Computing, Optimization, and Decision Technologies, 37*, Chap 15, Springer, New York.

Carey, C. (1998, January 1). *Force protection plus*. Security Solution.com. Retrieved September 10, 2008, from http://securitysolutions.com/mag/security_force_protection_plus/

Carroll, D., Everett, H.R., Gilbreath, G., Mullens, K., & Space And Naval Warfare Systems Center San Diego, CA. (2002). *Extending mobile security robots to force protection mission*s. Ft. Belvoir, VA: Defense Technical Information Center.

Chambers, C.G. (1984, May). Protection from the outside in. *Security Management*, *28*(5), 67.

Charles, M. (2001). Infrastructure security is a top priority in Congress. *Civil Engineering*, *71*(12), 12.

Conrow, E.H. (1995, Summer). Some long-term issues and impediments affecting military systems acquisition reform. *Acquisition Review Quarterly*, *2*(3), 199-212.

Conrow, E.H. (2005, February). Risk management for systems of systems. *Crosstalk*. Retrieved October 21, 2008, from http://www.stsc.hill.sf.mil/ crosstalk/2005

Coutteau, C.G., Long, J.E., & Bentzel, T.F. (2006, April). Active protection systems (APS) for the U.S. Army. *Military Technology, 30*(4), 64.

Creel, R., & Ellison, B. (2008, June 5). System-of-systems influences on acquisition strategy development. Pittsburg, PA: Software Engineering Institute, Carnegie Mellon University.

D'Angelo, A.F., Houglan, D.H., & Ruckwardt, E. (2007, December). *The need for a strategic approach to contingency contracting* (Master's Thesis). Monterey, CA: Naval Postgraduate School.

Department of Defense. (2003, August 18). DoD antiterrorism/force protection (AT/FP) program (DoD Directive 2000.12). Washington, DC: Author.

Department of Defense. (2004). *Defense acquisition guidebook*. Retrieved from DAU, Defense Acquisition Guidebook website: http://akss.dau.mil/dag

Department of Defense. (2006, October 2). DoD antiterrorism (AT) standards (DoD Instruction 2000.16). Washington, DC: Author.

Department of Defense. (2008, February 1). *Executive summary: Joint Capability Technology Demonstration (JCTD) Program—Practical Operating Guidelines (POG) Narrative Description*. (Vers. 1.0). Powerpoint Presentation. Washington, DC: Author.

Department of Homeland Security. (2007a). Protecting critical infrastructures and key assets. In *National Strategy for Homeland Security* (29-362007). Retrieved June 10, 2008, from http://www.whitehouse.gov/homeland/book

Department of Homeland Security. (2007b). *Critical infrastructures and key resources sectors*. Retrieved July 13, 2008, from http://www.dhs.gov/xprevprot/programs/gc_ 1189168948944.shtm

Ellison, R. J., Goodenough, J., Weinstock, C., & Woody, C. (2008). *Survivability assurance for system of systems* (CMU/SEI-2008-TR-008). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University.

Endress, C. (2007, July). Critical infrastructure protection—Strategies and technologies. *Military Technology*, *31*(7), 79-80.

Esterbrook, S. (2007). Scale changes everything: Understanding the requirements for systems of systems. Keynote address. 6th IEEE International Conference on COTS-based Software Systems, Baniff, CA.

Fastabend, D.A., & Simpson, R.H. (2004, February). Adapt or die. *Army*, *54*(2), 14-23.

Forward operating base. (2008). *Wikipedia*. Retrieved July 14, 2008, from http://en.wikipedia.org/w/index.php?title=Forward_operating_base&oldid=217364387

Franklin, S., & Graesser, A. (1996, June 19). *Is it an agent, or just a program?: A taxonomy for autonomous agents*.. Retrieved July 13, 2008, from University of Memphis, Institute for Intelligent Systems Web site: http://www.msci.memphis.edu/~franklin/AgentProg.html

Freiter, S. (2007, July). Defense department aims at shared physical security architecture. *Security*, *44*(7), 56.

Goscinski, A., (1989). *Protection and security in distributed operating systems*. Canberra, ACT: University College, University of New South Wales, Dept. of Computer Science, Australian Defense Force Academy.

Gruber, T.R. (1995, November). Toward principles for the design of ontologies used for knowledge sharing. *International Journal of Human-Computer Studies, 43*(4-5), 907-928.

Guardian Six Headquarters. (2008, July 11). *JFPASS joint capabilities technology demonstration (JCTD) Management and transition plan (MTP)*. (Vers. 1.1). Washington, DC: Author.

Gupta, K., Zang, M.A., Gray, A., Aha, D.W., Kriege, J., & Pohl, J. (2007). Enabling the interoperability of large-scale legacy systems. In *Proceedings of the Twentieth Innovative Applications of Artificial Intelligence Conference*. Retrieved July 13, 2008, from http://works.bepress.com/jpohl/72

Hart, B.L. (1967). *Strategy* (2nd ed). London: Meridian Books.

Heitman, R. (1997, November 17). Force protection office forms at electronic systems center. *Air Force News Service*.

Howard, M. (2007, November). Lessons learned from five years of building more secure software. *MSDN Magazine*.

Idziak, S. (2006, January 26). Threat reduction agency opens new headquarters. *US Fed News Service, Including US State News*. Retrieved September 10, 2008, from http://proquest. umi.com/pqdweb?did=982176131&Fmt=7&clientId=65345&RQT=309&VName=PQD

Joyce, L. (2005, June). Military apps drive simulation tools. *R & D*, *47*(6), 16.

Kent, G. (2004). *Force protection*. New York: Delacorte Press.

Kovacich, G.L., & Halibozek, E.P. (2006). *Security metrics management: How to measure the costs and benefits of security*. Burlington, MA: Butterworth-Heinemann.

Lama, K. (2007, October 24). *Joint Forces Protection Advanced Security System (JFPASS) FY08 JCTD candidate*. Briefing. Washington, DC: Author.

Lin, G.Y., Luby, R.E., Jr, & Wang, K-Y. (2004, December). New model for military operations. *ORMS Today*, *31*(6), 23-26.

London Stock Exchange. (2007, April 30). ViaLogy PLC business update. London: Author..

Maier, M. (1998). Architecting principles for systems of systems. *Systems Engineering 1*(4), 267-84.

McCrie, R.D. (2006). *Security operations management*. San Diego, CA: Elsevier.

Melcher, D.F. (2005, October). Making the transition from the current to the future force. *Army*, *55*(10), 187-196.

Merklinghaus, D-P. (2007). Impervious force protection for the future. *NATO's Nations and Partners for Peace*, (3), 72-79.

Montgomery, J. S., & Chin, E.S. (2008). Protecting the future force. *Military Technology*, *32*(2), 110.

Muradian, V. (1999, April 19). Gansler: New techniques needed for consolidation. *Defense Daily*, *202*(13), 1-8.

Personal protection solutions for today have armed conflicts. (2006). *Military Technology*, *30*(6), 150-154. Retrieved September 10, 2008, from http://proquest.umi.com/pqdweb ?did=1074989351&Fmt=7&clientId=65345&RQT=309&VName=PQD

Pohl, J. (2004). Interoperability and the need for intelligent software. In *Proceedings of the 2004 ONR Decision-Support Workshop Series: Interoperability*. 1-26.

Pohl, J. (2005). Intelligent software systems in historical context. *Decision Support Systems in Agent-Based Intelligent Environments*, 3-34.

Pohl, J., (2008, October 21). Intelligent software systems for military supply chain management, collaborative agent design research center (CADRC) California Polytechnic State University (Cal Poly, San Luis Obispo). Briefing & PowerPoint. Monterey, CA: Naval Postgraduate School.

Pohl, K.J., & Pohl, J. (2008). Perspective models: A mechanism for achieving interoperability among expressive, personalized domain views. In *Proceedings of InterSymp-2008: The 20th International Conference on Systems Research, Informatics and Cybernetics*. Baden-Baden, Germany.

Recon truck marketed for military base security. (2002, May). *National Defense*.

Reid, J. (2007, June). Securing the critical national infrastructure. *RUSI Journal*, *152*(3), 14-16.

Rhodes, J.E. (1998, January). Every Marine an innovator. *Marine Corps Gazette*, *82*(1), 40-44.

Rhodes, J.E. (2001, October). The U.S. and the changing nature of warfare. *Defense & Foreign Affairs Strategic Policy*, *29*(10), 11-12.

Roosevelt, A. (2004, June 3). Army identifies capability gaps, seeks solutions. *Defense Daily*, 222(45), 1. Retrieved September 10, 2008, from http://proquest.umi.com/pqdweb?did=645871471&Fmt=7&clientId=65345 &RQT=309&VName=PQD

Schwartz, J. (2007, September 12). Who needs hackers? *New York Times*.

Seo, Y., Ankolekar, A., & Sycara, K. (2004, March). Feature selection for extracting semantically rich words (CMU-RI-TR-04-18). Pittsburgh, PA: Robotics Institute, Carnegie Mellon University.

Shoop, B., Johnston, M., Goehring, R., Moneyhun, J., & Skibba, B. (2006). Mobile Detection Assessment and Response Systems (MDARS): A force protection physical security operational success. In *Proceedings*of *SPIE*, The International Society for Optical Engineering (pp. 6,230-6,280): SPIE.

Sinnreich, R.H. (2004, April). Training an adaptive military force to standard. *Army*, *54*(4), 12.

Tiron, R. (2004, May). Warfare by remote control. *National Defense,* 88(606), 26-28.

United States Army Test and Evaluation Command. (2008, October 14). *Integrated Assessment Plan (IAP) For the Joint Force Protection Advanced Security System (JFPASS) Joint Concept Technology Demonstration (JCTD)*. , Alexandria, VA: Author.

US DoD announces new joint capability technology demonstrations. (2008, January 30). *Defense Systems Daily*, 1-3.

Ward, M.C., Elm, J. P., & Kushner, S. (2006). Techniques for developing an acquisition strategy by profiling software risks (CMU/SEI-2006-TR-002). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University.

Appendix A. JFPASS Survey IRB Approval Memorandum

Naval Postgraduate School
Institutional Review Board (IRB)

21-Oct-08

From: LCDR Paul O'Connor, PhD
To: Senior Lecturer Raymond Franck
MAJ Mark McGovern

Subject: YOUR PROJECT: JOINT FORCES PROTECTION ADVANCE SECURITY SYSTEM UTILITY ASSESSMENT SURVEY

1. The NPS IRB is pleased to inform you that the NPS Institutional Review Board has approved your project (NPS IRB# NPS20090010-IR-EP7-A).
2. The NPS IRB was originally certified by BUMED on 26 July 2002 and has been re-certified until 30 August 2009.
3. This approval is valid for one year from this date. Please submit a copy of all records and consent forms to the Research and Sponsored Programs Office (Laura Ann Ekner-Price, Halligan Hall, Room 201B) at the conclusion of this project.
4. If your protocol changes at any time, you will need to resubmit your project proposal to the NPS IRB.

Under 32 CFR 219.116(d), the IRB finds that the requirement to describe procedures may be altered so that subjects receive the attached debriefing information after their participation.

Sincerely,

LCDR Paul O'Connor, PhD
Chair
NPS Institutional Review Board

THIS PAGE INTENTIONALLY LEFT BLANK

Appendix B. Desired Capabilities Relevance Survey Instructions

JOINT FORCES PROTECTION ADVANCED SECURITY SYSTEM (JFPASS) UTILITY ASSESSMENT SURVEY

Please fill in the chart, using the number scale provided, with your own opinion.

Request return at your earliest opportunity.

Introduction:

This survey will be used as a tool to measure the operational capability of the JFPASS in comparison to both the status quo (do nothing) and five competing systems. This survey is intended to provide a foundation of expert judgment for the establishment of a measure of operational utility. For the purpose of this project, this survey is meant to be all encompassing, but only a small part of the tests and studies being conducted within the JFPASS Joint. This survey will be distributed to persons with operational deployment experience via email and personal contact. Risk associated with this survey is deemed as minimal to any person who volunteers to participate. No personal information is requested or required and any information linking participants with this survey will be destroyed or deleted once numerical data is collected. Additionally, conclusions derived from the data collected from this survey will be encompassed into possible future studies of the JFPASS.

Purpose:

For the purpose of this survey, eight desired capabilities are to be assessed with respect to their contribution to successfully perform five key tasks. Your responses will then be used to formulate metrics that can be used to assess the relative importance of each of those capabilities. While not all capabilities will necessarily have direct relevance on a specific task, each task/capability should be weighted. As an operational expert in the force projection mission, we ask that you consider the relevance of the capability in relation to each specific task.

What we want from you:

Our specific project will analyze how each of the desired capabilities improves overall ability to provide effective force protection. Force protection is defined here as anything that enhances thwarting attempts on US life, property, or infrastructure.

We want your best judgment of how each of the capabilities in the table below contributes to the successful accomplishment of the five force protection tasks. We understand that your assessments are subjective and the return of the survey constitutes consent in your participation.

Definitions:

A listing and a brief description of the five key tasks and the eight desired capabilities are provided below.

Desired Capabilities:[1]

1. Near Real-TTime/Integrated/Interoperable, Comprehensive Land and Maritime-based Reg balanced Local Force Protection (FP) Systems; Common Operating Picture (COP) tailored to suit the user's information requirements and built from fused sensor and other information sources
2. Scalable FP area of interest to support a single integrated group (military and civilian)
3. Compliance with regional requirements (e.g. laws, regulations, SOFAs)
4. Suite of systems under a central core, ability to share information (voice data and video) with subordinate units, higher headquarters, and adjacent C2 nodes
5. Standardized core systems training, common baseline of equipment, interface, and training standards which reduces the total lifecycle cost of ownership and facilitates the plug and play use of components among the Services and our coalition partners
6. Internationally releasable system suite (between partner nations)
7. A decision aide to select a system suite for various applications/environments
8. CONOPS and TTPs developed for the employment of the integrated system-of-systems

Tasks: [2]

The JFPASS will be tested against the following tasks, according to each task description.

1. Detect: The JFPASS will demonstrate the ability to detect threats using an integrated system of sensors (including cameras, radar, and CBRNE detection). This will provide consistent detection probability results improved response both in the time required to recognize a threat and the ability to do so at greater distances from vital assets.
2. Assess: The JFPASS will integrate the sensors into an automated centrally controlled processing station(s), which will evaluate the input from each of the sensor systems. The JFPASS will automate the assessment process by comparing the nature of any anomaly detected by the JFPASS system with the current understanding of any known threat and the potential for the anomaly to become a threat (i.e., presence of explosive

---

[1] Guardian Six Headquarters. (2008, July 11). *JFPASS joint capabilities technology demonstration (JCTD) Management and transition plan (MTP)*. (Vers. 1.1). Washington, DC: Author. p. 19

[2] Ibid.

components or precursors). The JFPASS will then automatically provide the system operator with recommended courses of action.

3. Warn: The JFPASS will provide situational awareness and information for decision makers. An internet worked system of the JFPASS enabled units, bases and installations will disseminate warnings via a network in order to mitigate the effects of dispersed coordinated attacks.
4. Defend: The JFPASS will automate the defense actions by centrally managing the deployment of passive defensive measures and providing the local commander with situational awareness regarding the status of the defensive measures.
5. Recover: Although the JFPASS will not directly contribute to the recovery function, the synergistic effect of integration and automation within the other areas of the FP construct will help in resuming effective operations and provide a deterrent against further attacks.

Numerical Evaluation Scores: (Level importance of task from the operational perspective in relation to desired capability)[3]

5–Significantly impacts mission success
4–Enhances mission success
3–Impacts mission success
2–Minimal impact on mission success
1–No impact on mission success

HIGH

LEVEL OF IMPORTANCE

LOW

Every block should receive a numerical value, or will be assumed as no impact.

See example below on how to properly fill in the chart using the numerical scale listed above.

[3] Fowler, M. J. (2001, December). Acquisition strategies for aging aircraft: Modernizing the marine corps' CH-53 super stallion helicopter (Master's Thesis). Monterey, CA: NPS.

	Near Real Time / Integrated / Interoperable, Comprehensive Land and Maritime-based Reg balanced Local Force Protection (FP) Systems	Scalable FP area of interest to support a single mutually supportive group (military and civilian)	Compliance with regional requirements (e.g. laws, regulations, SOFAs)	Suite of systems under a central core	Standardized core systems training	Internationally releasable system suite (between partner nations)	A decision aide to select a system suite for various applications / environments	CONOPS and TTPs
DETECT	5	4	3	5	2	3	3	2
ASSESS	5	4	4	2	5	3	4	4
WARN	5	5	2	2	3	1	3	1
DEFEND	5	1	3	4	2	5	5	3
RECOVER	5	3	3	2	2	4	2	1

TASKS WEIGHTING IMPORTANCE[4] (Example Format)

REMEMBER: Each block should have a numerical value assigned.

Instructions for returning:

1-Download SURVEY FORM.doc and save as JFPASS_SURVEY to your desktop.

2-Attach saved doc's to email or mail / fax to: (**jbsymmes@nps.edu**)

Fax: ATTN: NPS JFPASS SURVEY, 831-444-9443
Mail: ATTN: NPS JFPASS SURVEY, 995 Newington St, Salinas CA 93906
POC: MAJ Mark McGovern (mtmcgove@nps.edu)

[4] Ibid.

Appendix C. Desired Capabilities Relevance Survey

JOINT FORCES PROTECTION ADVANCED SECURITY SYSTEM (JFPASS) UTILITY ASSESSMENT SURVEY

Please fill in the chart, using the number scale provided, with your own opinion.
Request return at your earliest opportunity.

	Near Real Time / Integrated / Interoperable, Comprehensive Land and Maritime-based Reg balanced Local Force Protection (FP) Systems	Scalable FP area of interest to support a single mutually supportive group (military and civilian)	Compliance with regional requirements (e.g. laws, regulations, SOFAs)	Suite of systems under a central core	Standardized core systems training	Internationally releasable system suite (between partner nations)	A decision aide to select a system suite for various applications / environments	CONOPS and TTPs
DETECT								
ASSESS								
WARN								
DEFEND								
RECOVER								

TASKS WEIGHTING IMPORTANCE[5]

Numerical Evaluation Scores: (Level importance of task from the operational perspective in relation to desired capability)[6]

5 – Significantly impacts mission success
4 – Enhances mission success
3 – Impacts mission success
2 – Minimal impact on mission success
1 – No impact on mission success

HIGH

LEVEL OF IMPORTANCE

LOW

REMEMBER: Each block should have a numerical value assigned.

Instructions for returning: **Note: Return of the survey constitutes consent.**

1-Download SURVEY FORM.doc and save as JFPASS_SURVEY to your desktop.

[5] Fowler, "Acquisition Strategies for Aging Aircraft.

[6] Ibid.

2-Attach saved doc's to email or mail / fax to: (**jbsymmes@nps.edu**)
Fax: ATTN: NPS JFPASS SURVEY, 831-444-9443
Mail: ATTN: NPS JFPASS SURVEY, 995 Newington St, Salinas CA 93906

Appendix D. JFPASS Survey Preference Rollup

1	Near Real Time	Scalable	SOFA Compliant	Suite of Systems Central Core	Standardized Training	Internationally Releasable	Decision Aide	CONOPS and TTPs
DETECT	5	4	3	5	2	3	3	2
ASSESS	5	4	4	2	5	3	4	4
WARN	5	5	2	2	3	1	3	1
DEFEND	5	1	3	4	2	5	5	3
RECOVER	5	3	3	2	2	4	2	1

2	Near Real Time	Scalable	SOFA Compliant	Suite of Systems Central Core	Standardized Training	Internationally Releasable	Decision Aide	CONOPS and TTPs
DETECT	5	4	3	5	2	3	3	2
ASSESS	5	4	4	2	5	3	4	4
WARN	5	5	2	2	3	1	3	1
DEFEND	5	1	3	4	2	5	5	3
RECOVER	5	3	3	2	2	4	2	1

3	Near Real Time	Scalable	SOFA Compliant	Suite of Systems Central Core	Standardized Training	Internationally Releasable	Decision Aide	CONOPS and TTPs
DETECT	4	2	1	3	2	2	1	2
ASSESS	4	3	1	3	2	2	3	2
WARN	4	5	1	4	2	3	3	2
DEFEND	4	4	1	4	2	2	2	2
RECOVER	4	2	1	3	2	2	1	2

4	Near Real Time	Scalable	SOFA Compliant	Suite of Systems Central Core	Standardized Training	Internationally Releasable	Decision Aide	CONOPS and TTPs
DETECT	4	2	1	2	3	1	5	4
ASSESS	4	3	1	2	4	2	4	4
WARN	4	5	1	2	5	3	3	5
DEFEND	4	4	1	2	2	4	2	2
RECOVER	4	2	1	2	1	5	1	1

5	Near Real Time	Scalable	SOFA Compliant	Suite of Systems Central Core	Standardized Training	Internationally Releasable	Decision Aide	CONOPS and TTPs
DETECT	5	5	3	5	4	4	3	2
ASSESS	5	5	3	5	4	2	3	4
WARN	5	3	2	4	2	2	3	2
DEFEND	4	4	2	4	3	2	2	4
RECOVER	4	3	2	2	3	2	1	1

6	Near Real Time	Scalable	SOFA Compliant	Suite of Systems Central Core	Standardized Training	Internationally Releasable	Decision Aide	CONOPS and TTPs
DETECT	5	5	3	5	3	5	5	3
ASSESS	5	5	3	3	3	3	5	3
WARN	5	5	3	5	3	5	5	3
DEFEND	5	5	3	5	3	5	5	3
RECOVER	5	3	1	3	3	2	5	1

7	Near Real Time	Scalable	SOFA Compliant	Suite of Systems Central Core	Standardized Training	Internationally Releasable	Decision Aide	CONOPS and TTPs
DETECT	4	4	4	4	4	3	4	4
ASSESS	3	4	4	4	4	3	3	4
WARN	3	3	4	3	3	3	3	4
DEFEND	3	2	4	2	3	3	2	3
RECOVER	2	2	4	2	2	2	2	2

8	Near Real Time	Scalable	SOFA Compliant	Suite of Systems Central Core	Standardized Training	Internationally Releasable	Decision Aide	CONOPS and TTPs
DETECT	4	4	3	5	5	5	5	4
ASSESS	5	4	4	5	5	4	5	4
WARN	4	5	3	5	4	4	4	4
DEFEND	3	2	2	3	4	3	2	4
RECOVER	3	2	2	3	4	3	2	4

9	Near Real Time	Scalable	SOFA Compliant	Suite of Systems Central Core	Standardized Training	Internationally Releasable	Decision Aide	CONOPS and TTPs
DETECT	4	4	2	5	5	5	5	5
ASSESS	5	4	4	5	5	3	5	3
WARN	4	5	3	5	4	3	2	3
DEFEND	3	2	2	3	3	2	2	3
RECOVER	2	2	2	2	3	2	2	3

10	Near Real Time	Scalable	SOFA Compliant	Suite of Systems Central Core	Standardized Training	Internationally Releasable	Decision Aide	CONOPS and TTPs
DETECT	5	4	1	3	5	1	5	5
ASSESS	5	4	1	3	5	1	5	5
WARN	5	4	1	3	5	1	5	5
DEFEND	5	4	1	3	5	1	5	5
RECOVER	5	4	1	3	5	1	5	5

11	Near Real Time	Scalable	SOFA Compliant	Suite of Systems Central Core	Standardized Training	Internationally Releasable	Decision Aide	CONOPS and TTPs
DETECT	5	5	4	5	3	2	3	4
ASSESS	4	3	3	5	3	2	4	3
WARN	5	5	2	5	3	2	5	4
DEFEND	4	3	3	5	3	2	5	3
RECOVER	4	2	2	4	3	2	4	2

12	Near Real Time	Scalable	SOFA Compliant	Suite of Systems Central Core	Standardized Training	Internationally Releasable	Decision Aide	CONOPS and TTPs
DETECT	5	4	5	3	4	5	4	3
ASSESS	3	3	3	5	5	3	5	2
WARN	4	2	4	4	3	4	3	5
DEFEND	2	5	2	2	2	2	2	4
RECOVER	1	1	1	1	1	1	1	1

13	Near Real Time	Scalable	SOFA Compliant	Suite of Systems Central Core	Standardized Training	Internationally Releasable	Decision Aide	CONOPS and TTPs
DETECT	5	4	2	5	5	5	5	5
ASSESS	5	4	4	5	5	5	5	5
WARN	5	4	4	5	5	5	5	5
DEFEND	5	5	5	5	5	5	5	5
RECOVER	2	1	1	1	1	1	1	1

14	Near Real Time	Scalable	SOFA Compliant	Suite of Systems Central Core	Standardized Training	Internationally Releasable	Decision Aide	CONOPS and TTPs
DETECT	5	4	2	4	4	3	4	3
ASSESS	3	4	2	4	3	3	3	3
WARN	4	5	2	4	3	3	4	3
DEFEND	5	3	2	3	3	3	3	3
RECOVER	2	3	2	2	3	3	3	3

15	Near Real Time	Scalable	SOFA Compliant	Suite of Systems Central Core	Standardized Training	Internationally Releasable	Decision Aide	CONOPS and TTPs
DETECT	5	5	1	5	4	3	2	2
ASSESS	5	4	4	5	5	3	2	3
WARN	5	4	3	5	5	4	3	2
DEFEND	5	4	4	5	4	4	2	4
RECOVER	5	2	1	4	4	1	2	3

16	Near Real Time	Scalable	SOFA Compliant	Suite of Systems Central Core	Standardized Training	Internationally Releasable	Decision Aide	CONOPS and TTPs
DETECT	5	4	3	5	2	3	3	2
ASSESS	5	4	3	3	5	2	3	4
WARN	5	4	2	2	3	1	3	3
DEFEND	5	2	3	5	3	5	5	2
RECOVER	5	2	3	2	3	4	2	3

17	Near Real Time	Scalable	SOFA Compliant	Suite of Systems Central Core	Standardized Training	Internationally Releasable	Decision Aide	CONOPS and TTPs
DETECT	5	5	3	3	3	2	4	2
ASSESS	4	2	2	3	2	2	3	1
WARN	5	2	3	3	2	2	4	1
DEFEND	4	4	2	3	3	2	3	2
RECOVER	4	1	2	2	2	2	3	1

18	Near Real Time	Scalable	SOFA Compliant	Suite of Systems Central Core	Standardized Training	Internationally Releasable	Decision Aide	CONOPS and TTPs
DETECT	5	5	4	4	5	3	5	3
ASSESS	5	5	5	4	5	3	4	3
WARN	5	5	4	5	5	3	3	3
DEFEND	5	5	3	3	5	3	5	3
RECOVER	5	3	4	2	5	3	2	3

19	Near Real Time	Scalable	SOFA Compliant	Suite of Systems Central Core	Standardized Training	Internationally Releasable	Decision Aide	CONOPS and TTPs
DETECT	5	1	5	4	3	3	4	5
ASSESS	3	3	4	4	3	5	5	1
WARN	4	5	5	1	4	5	5	1
DEFEND	5	4	3	3	1	5	3	3
RECOVER	3	5	3	5	1	3	4	4

20	Near Real Time	Scalable	SOFA Compliant	Suite of Systems Central Core	Standardized Training	Internationally Releasable	Decision Aide	CONOPS and TTPs
DETECT	5	5	3	3	4	2	2	1
ASSESS	5	4	2	3	4	2	4	1
WARN	5	5	3	3	3	2	3	1
DEFEND	5	5	3	3	4	2	2	1
RECOVER	5	3	2	3	3	2	1	1

21	Near Real Time	Scalable	SOFA Compliant	Suite of Systems Central Core	Standardized Training	Internationally Releasable	Decision Aide	CONOPS and TTPs
DETECT	5	2	2	3	2	2	2	2
ASSESS	4	5	2	2	1	2	2	1
WARN	5	4	2	3	2	2	2	2
DEFEND	5	3	2	3	2	2	2	1
RECOVER	4	5	2	2	1	2	2	1

22	Near Real Time	Scalable	SOFA Compliant	Suite of Systems Central Core	Standardized Training	Internationally Releasable	Decision Aide	CONOPS and TTPs
DETECT	5	3	2	3	2	1	2	1
ASSESS	4	2	2	3	2	1	1	1
WARN	5	3	2	2	2	1	2	1
DEFEND	4	4	2	2	2	1	2	1
RECOVER	3	1	1	1	2	1	1	1

23	Near Real Time	Scalable	SOFA Compliant	Suite of Systems Central Core	Standardized Training	Internationally Releasable	Decision Aide	CONOPS and TTPs
DETECT	5	5	3	2	2	3	3	2
ASSESS	5	5	2	2	2	1	2	2
WARN	5	4	3	2	2	2	3	2
DEFEND	5	5	2	2	2	2	2	2
RECOVER	4	3	1	2	2	1	1	2

24	Near Real Time	Scalable	SOFA Compliant	Suite of Systems Central Core	Standardized Training	Internationally Releasable	Decision Aide	CONOPS and TTPs
DETECT	5	4	3	5	2	3	3	2
ASSESS	5	4	4	2	5	3	4	4
WARN	5	5	2	2	3	1	3	1
DEFEND	5	1	3	4	2	4	5	3
RECOVER	5	4	3	2	2	5	2	1

25	Near Real Time	Scalable	SOFA Compliant	Suite of Systems Central Core	Standardized Training	Internationally Releasable	Decision Aide	CONOPS and TTPs
DETECT	5	4	2	4	5	2	1	2
ASSESS	5	4	2	4	5	2	2	4
WARN	5	4	2	4	5	2	2	1
DEFEND	5	4	2	4	5	1	5	1
RECOVER	5	4	2	4	5	2	2	1

26	Near Real Time	Scalable	SOFA Compliant	Suite of Systems Central Core	Standardized Training	Internationally Releasable	Decision Aide	CONOPS and TTPs
DETECT	5	4	2	4	5	2	1	2
ASSESS	5	4	2	4	5	2	2	4
WARN	5	4	2	4	5	2	2	1
DEFEND	5	4	2	4	5	1	5	1
RECOVER	5	4	2	4	5	2	2	1

27	Near Real Time	Scalable	SOFA Compliant	Suite of Systems Central Core	Standardized Training	Internationally Releasable	Decision Aide	CONOPS and TTPs
DETECT	5	4	3	5	3	3	3	4
ASSESS	4	3	5	3	2	2	2	3
WARN	4	3	4	3	2	2	2	3
DEFEND	5	4	5	4	5	4	3	4
RECOVER	4	3	3	3	2	2	2	2

28	Near Real Time	Scalable	SOFA Compliant	Suite of Systems Central Core	Standardized Training	Internationally Releasable	Decision Aide	CONOPS and TTPs
DETECT	5	5	1	3	4	2	4	2
ASSESS	5	5	1	3	4	2	3	2
WARN	5	5	1	3	4	2	3	2
DEFEND	5	5	2	3	4	2	4	2
RECOVER	5	5	1	3	4	2	2	2

29	Near Real Time	Scalable	SOFA Compliant	Suite of Systems Central Core	Standardized Training	Internationally Releasable	Decision Aide	CONOPS and TTPs
DETECT	5	5	2	4	2	2	4	3
ASSESS	5	4	2	3	2	2	3	3
WARN	5	5	2	3	2	2	3	3
DEFEND	5	5	2	4	2	2	4	3
RECOVER	5	3	2	3	2	2	3	3

30	Near Real Time	Scalable	SOFA Compliant	Suite of Systems Central Core	Standardized Training	Internationally Releasable	Decision Aide	CONOPS and TTPs
DETECT	5	5	2	3	4	2	4	2
ASSESS	5	5	2	3	4	2	4	2
WARN	5	5	2	3	4	2	4	2
DEFEND	5	5	2	3	4	2	5	2
RECOVER	5	2	1	3	4	1	2	2

31	Near Real Time	Scalable	SOFA Compliant	Suite of Systems Central Core	Standardized Training	Internationally Releasable	Decision Aide	CONOPS and TTPs
DETECT	5	5	2	3	2	1	4	2
ASSESS	5	4	2	3	2	1	4	2
WARN	3	4	2	3	2	1	4	2
DEFEND	5	5	2	3	2	1	4	2
RECOVER	2	3	1	3	1	1	2	2

32	Near Real Time	Scalable	SOFA Compliant	Suite of Systems Central Core	Standardized Training	Internationally Releasable	Decision Aide	CONOPS and TTPs
DETECT	5	4	3	5	3	3	3	2
ASSESS	5	4	4	4	3	3	4	2
WARN	5	5	2	2	2	3	3	1
DEFEND	5	3	3	2	5	1	3	3
RECOVER	5	2	3	2	2	4	2	1

33	Near Real Time	Scalable	SOFA Compliant	Suite of Systems Central Core	Standardized Training	Internationally Releasable	Decision Aide	CONOPS and TTPs
DETECT	5	5	2	4	4	2	4	3
ASSESS	5	4	2	3	3	2	3	2
WARN	5	5	2	3	3	2	3	3
DEFEND	5	5	2	4	4	2	4	3
RECOVER	2	2	2	2	2	2	2	2

34	Near Real Time	Scalable	SOFA Compliant	Suite of Systems Central Core	Standardized Training	Internationally Releasable	Decision Aide	CONOPS and TTPs
DETECT	5	5	2	4	4	2	2	1
ASSESS	5	5	2	4	4	2	1	1
WARN	5	5	2	4	4	2	2	1
DEFEND	5	5	2	4	4	2	1	1
RECOVER	5	3	2	4	4	2	2	1

35	Near Real Time	Scalable	SOFA Compliant	Suite of Systems Central Core	Standardized Training	Internationally Releasable	Decision Aide	CONOPS and TTPs
DETECT	5	5	3	4	4	4	2	1
ASSESS	5	4	3	3	3	2	2	1
WARN	5	5	2	3	4	3	1	1
DEFEND	5	5	3	3	4	3	2	1
RECOVER	5	4	2	3	3	1	1	1

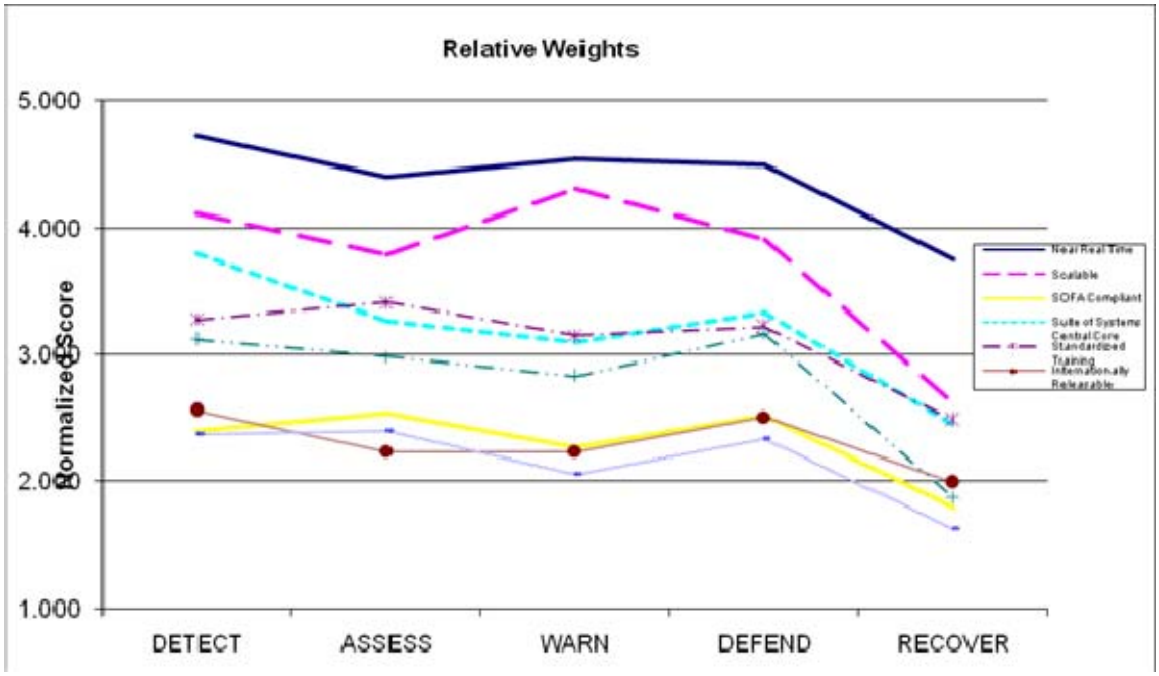
36	Near Real Time	Scalable	SOFA Compliant	Suite of Systems Central Core	Standardized Training	Internationally Releasable	Decision Aide	CONOPS and TTPs
DETECT	5	5	3	4	4	3	2	2
ASSESS	5	4	2	3	4	2	2	2
WARN	5	5	3	2	4	1	2	2
DEFEND	5	5	3	3	4	3	2	2
RECOVER	4	3	2	2	3	1	1	1

37	Near Real Time	Scalable	SOFA Compliant	Suite of Systems Central Core	Standardized Training	Internationally Releasable	Decision Aide	CONOPS and TTPs
DETECT	5	5	3	4	3	3	4	2
ASSESS	4	4	2	3	3	3	3	2
WARN	5	5	2	3	3	3	2	2
DEFEND	5	5	3	4	3	3	4	2
RECOVER	3	2	2	2	2	2	2	2

38	Near Real Time	Scalable	SOFA Compliant	Suite of Systems Central Core	Standardized Training	Internationally Releasable	Decision Aide	CONOPS and TTPs
DETECT	5	4	4	4	4	3	4	2
ASSESS	4	3	3	4	4	3	3	2
WARN	5	5	3	4	4	3	3	1
DEFEND	5	5	4	4	4	3	4	2
RECOVER	3	2	2	2	2	2	2	1

39	Near Real Time	Scalable	SOFA Compliant	Suite of Systems Central Core	Standardized Training	Internationally Releasable	Decision Aide	CONOPS and TTPs
DETECT	5	4	2	4	3	3	3	3
ASSESS	4	4	3	4	3	3	2	2
WARN	5	5	3	4	3	3	3	2
DEFEND	4	5	5	5	3	4	2	3
RECOVER	3	3	2	3	2	3	2	2

Appendix E. Survey Preference Results



This graph shows the WF preferences of operational capabilities graphed according to the five standard key tasks along the X-axis. This clearly shows a preference for near real-time capability. This graph also shows how the WFs consider the recovery phase to be the least important key task.

THIS PAGE INTENTIONALLY LEFT BLANK

Appendix F. Polar Graph of Standard Deviation of Near Real-time Results

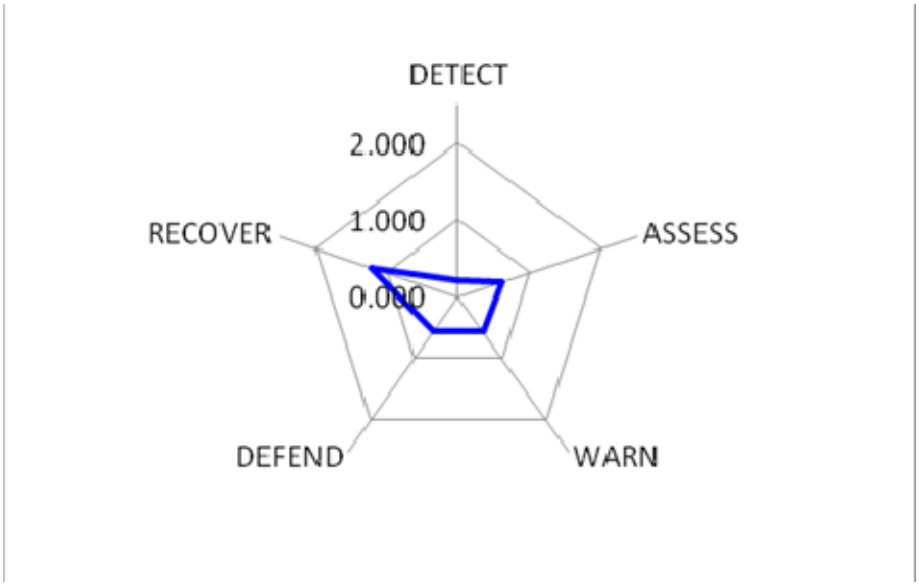


Figure F-1. Near Real-time

This graph shows the extremely low deviation in responses for the importance of the near real time operational capability. Specifically, the detection phase was the key task that had the least variability in responses.

THIS PAGE INTENTIONALLY LEFT BLANK

Appendix G. Measure of Effectiveness Calculation Tool 1

Measure of Effectiveness Rating

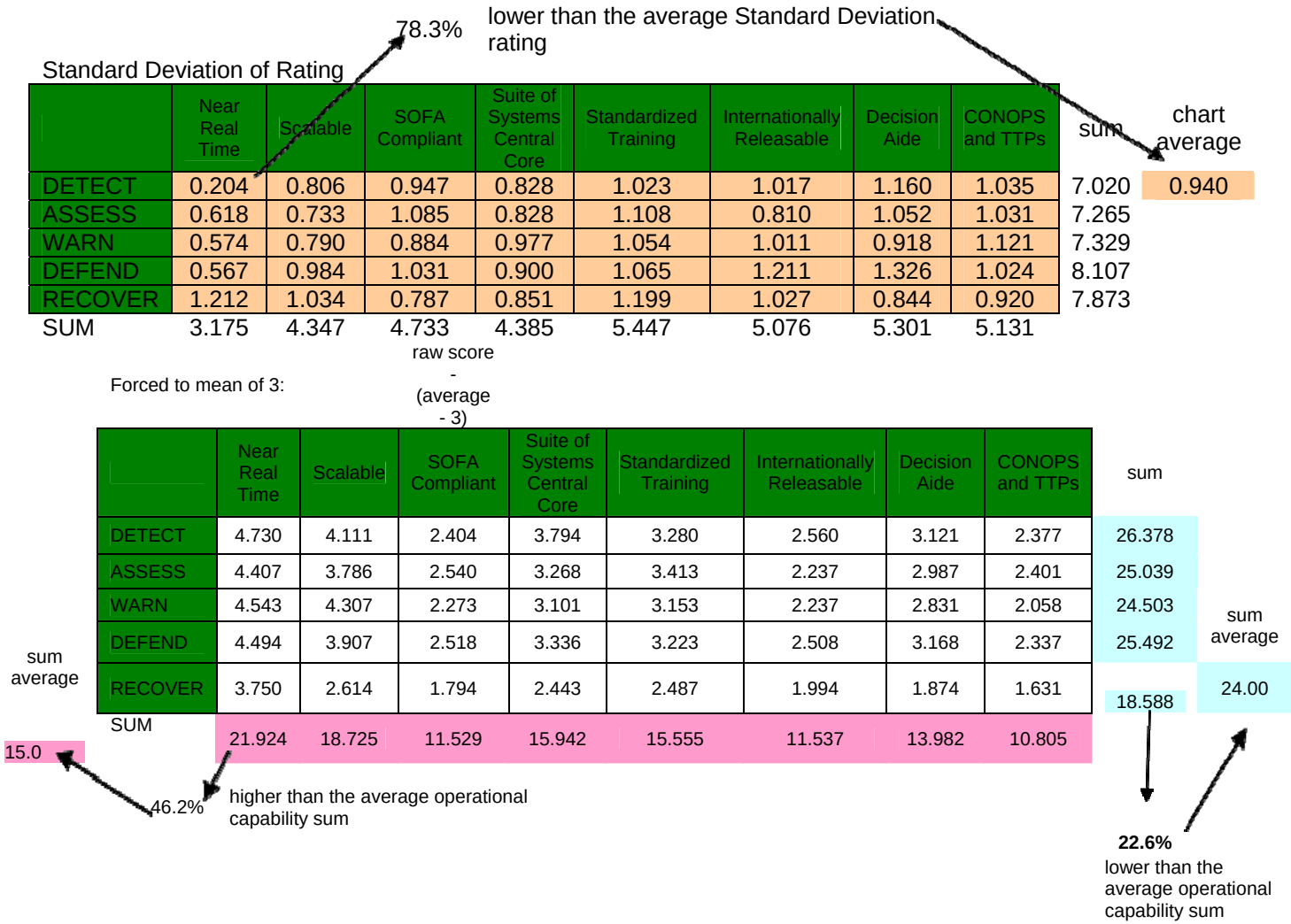
Engineers / Contractors Performance Measure		1	1	1	1	1	1	1	1
		Near Real Time	Scalable	SOFA Compliant	Suite of Systems Central Core	Standardized Training	Internationally Releasable	Decision Aide	CONOPS and TTPs
Operational Users Performance Preference Rating	DETECT	3.87	3.50	2.93	3.23	3.06	2.82	3.17	2.75
	ASSESS	3.76	3.39	2.98	3.05	3.10	2.71	3.12	2.76
	WARN	3.81	3.56	2.72	3.00	3.01	2.71	2.91	2.65
	DEFEND	3.79	3.26	2.80	3.07	3.04	2.80	3.02	2.74
	RECOVER	3.21	2.83	2.39	2.61	2.62	2.46	2.42	2.34
	SUM	18.5	16.6	13.8	15.0	14.8	13.5	14.6	13.2
Weighted Sum Across All Capabilities		18.5	16.6	13.8	15.0	14.8	13.5	14.6	13.2

Overall, MOE Weighted Across All Capabilities	120.0

In order to determine an overall measure of effectiveness score, we created a field to be filled in once performance data becomes available. The chart above multiplies that performance score by the weighted preference sum derived from our surveys. The total of all these preferences across all operational capabilities gives an overall, weighted measure of effectiveness score. This tool could be very useful for analyzing how relative changes in specific areas of performance affect the overall system effectiveness. This tool drives the polar measure of effectiveness graph seen in Figure 6.

THIS PAGE INTENTIONALLY LEFT BLANK

Appendix H. Measure of Effectiveness Calculation Tool 2



	Near Real Time	Scalable	SOFA Compliant	Suite of Systems Central Core	Standardized Training	Internationally Releasable	Decision Aide	CONOPS and TTPs	sum	chart average
DETECT	0.204	0.806	0.947	0.828	1.023	1.017	1.160	1.035	7.020	0.940
ASSESS	0.618	0.733	1.085	0.828	1.108	0.810	1.052	1.031	7.265	
WARN	0.574	0.790	0.884	0.977	1.054	1.011	0.918	1.121	7.329	
DEFEND	0.567	0.984	1.031	0.900	1.065	1.211	1.326	1.024	8.107	
RECOVER	1.212	1.034	0.787	0.851	1.199	1.027	0.844	0.920	7.873	
SUM	3.175	4.347	4.733	4.385	5.447	5.076	5.301	5.131		

	Near Real Time	Scalable	SOFA Compliant	Suite of Systems Central Core	Standardized Training	Internationally Releasable	Decision Aide	CONOPS and TTPs	sum	sum average
DETECT	4.730	4.111	2.404	3.794	3.280	2.560	3.121	2.377	26.378	
ASSESS	4.407	3.786	2.540	3.268	3.413	2.237	2.987	2.401	25.039	
WARN	4.543	4.307	2.273	3.101	3.153	2.237	2.831	2.058	24.503	
DEFEND	4.494	3.907	2.518	3.336	3.223	2.508	3.168	2.337	25.492	
RECOVER	3.750	2.614	1.794	2.443	2.487	1.994	1.874	1.631	18.588	24.00
SUM	21.924	18.725	11.529	15.942	15.555	11.537	13.982	10.805		

These tables point out the statistically significant survey responses. The low standard deviation of near real-time importance during the detection phase is highlighted in the top chart. The bottom chart shows both the importance of near real-time detection and the reduced importance of the recovery phase to the WF. To show the order of magnitude of these three significant data points, each has been compared with a comparable overall average.

2003 - 2008 Sponsored Research Topics

Acquisition Management

- Acquiring Combat Capability via Public-Private Partnerships (PPPs)
- BCA: Contractor vs. Organic Growth
- Defense Industry Consolidation
- EU-US Defense Industrial Relationships
- Knowledge Value Added (KVA) + Real Options (RO) Applied to Shipyard Planning Processes
- Managing Services Supply Chain
- MOSA Contracting Implications
- Portfolio Optimization via KVA + RO
- Private Military Sector
- Software Requirements for OA
- Spiral Development
- Strategy for Defense Acquisition Research
- The Software, Hardware Asset Reuse Enterprise (SHARE) repository

Contract Management

- Commodity Sourcing Strategies
- Contracting Government Procurement Functions
- Contractors in 21st Century Combat Zone
- Joint Contingency Contracting
- Model for Optimizing Contingency Contracting Planning and Execution
- Navy Contract Writing Guide
- Past Performance in Source Selection
- Strategic Contingency Contracting
- Transforming DoD Contract Closeout
- USAF Energy Savings Performance Contracts
- USAF IT Commodity Council
- USMC Contingency Contracting

Financial Management

- Acquisitions via leasing: MPS case
- Budget Scoring
- Budgeting for Capabilities Based Planning
- Capital Budgeting for DoD
- Energy Saving Contracts/DoD Mobile Assets
- Financing DoD Budget via PPPs
- Lessons from Private Sector Capital Budgeting for DoD Acquisition Budgeting Reform
- PPPs and Government Financing
- ROI of Information Warfare Systems
- Special Termination Liability in MDAPs
- Strategic Sourcing
- Transaction Cost Economics (TCE) to Improve Cost Estimates

Human Resources

- Indefinite Reenlistment
- Individual Augmentation
- Learning Management Systems
- Moral Conduct Waivers and First-tem Attrition
- Retention
- The Navy's Selective Reenlistment Bonus (SRB) Management System
- Tuition Assistance

Logistics Management

- Analysis of LAV Depot Maintenance
- Army LOG MOD
- ASDS Product Support Analysis
- Cold-chain Logistics
- Contractors Supporting Military Operations
- Diffusion/Variability on Vendor Performance Evaluation
- Evolutionary Acquisition
- Lean Six Sigma to Reduce Costs and Improve Readiness

- Naval Aviation Maintenance and Process Improvement (2)
- Optimizing CIWS Lifecycle Support (LCS)
- Outsourcing the Pearl Harbor MK-48 Intermediate Maintenance Activity
- Pallet Management System
- PBL (4)
- Privatization-NOSL/NAWCI
- RFID (6)
- Risk Analysis for Performance-based Logistics
- R-TOC Aegis Microwave Power Tubes
- Sense-and-Respond Logistics Network
- Strategic Sourcing

Program Management

- Building Collaborative Capacity
- Business Process Reengineering (BPR) for LCS Mission Module Acquisition
- Collaborative IT Tools Leveraging Competence
- Contractor vs. Organic Support
- Knowledge, Responsibilities and Decision Rights in MDAPs
- KVA Applied to Aegis and SSDS
- Managing the Service Supply Chain
- Measuring Uncertainty in Eared Value
- Organizational Modeling and Simulation
- Public-Private Partnership
- Terminating Your Own Program
- Utilizing Collaborative and Three-dimensional Imaging Technology

A complete listing and electronic copies of published research are available on our website: www.acquisitionresearch.org

THIS PAGE INTENTIONALLY LEFT BLANK

ACQUISITION RESEARCH PROGRAM
GRADUATE SCHOOL OF BUSINESS & PUBLIC POLICY
NAVAL POSTGRADUATE SCHOOL
555 DYER ROAD, INGERSOLL HALL
MONTEREY, CALIFORNIA 93943

www.acquisitionresearch.org